

~~SECRET//NOFORN~~

Report No. DODIG-2016-026



INSPECTOR GENERAL

U.S. Department of Defense

November 24, 2015

~~(U//FOUO)~~ Combat Mission Teams and Cyber Protection Teams Lacked Adequate Capabilities and Facilities to Perform Missions

Classified By: Carol N. Gorman, Assistant Inspector General
Derived From: Multiple Sources
Declassify On: 20461411

Report 35 of 50

INTEGRITY ★ EFFICIENCY ★ ACCOUNTABILITY ★ EXCELLENCE

~~SECRET//NOFORN~~

INTEGRITY ★ EFFICIENCY ★ ACCOUNTABILITY ★ EXCELLENCE

Mission

Our mission is to provide independent, relevant, and timely oversight of the Department of Defense that supports the warfighter; promotes accountability, integrity, and efficiency; advises the Secretary of Defense and Congress; and informs the public.

Vision

Our vision is to be a model oversight organization in the Federal Government by leading change, speaking truth, and promoting excellence—a diverse organization, working together as one professional team, recognized as leaders in our field.



Fraud, Waste & Abuse

HOTLINE

Department of Defense

dodig.mil/hotline | 800.424.9098

For more information about whistleblower protection, please see the inside back cover.



Results in Brief

(U//~~FOUO~~) Combat Mission Teams and Cyber Protection Teams Lacked Adequate Capabilities and Facilities to Perform Missions

November 24, 2015

(U) Objective

(U) We determined whether Cyber Mission Force (CMF) teams had adequate facilities, equipment, and capabilities to effectively perform missions.

(U) Finding

~~(S//REL TO USA, FVEY)~~
ARMY; NAVY; USAF; USMC: (b)(1), Sec. 1.4(g)

- ~~(S//REL TO USA, FVEY)~~
ARMY; NAVY; USAF; USMC: (b)(1), Sec. 1.4(g)

- ~~(S//REL TO USA, FVEY)~~
ARMY; NAVY; USAF; USMC: (b)(1), Sec. 1.4(g)

- ~~(S//REL TO USA, FVEY)~~
ARMY; NAVY; USAF; USMC: (b)(1), Sec. 1.4(g)

(U) Finding (cont'd)

- (U//~~FOUO~~) Army Cyber Command did not provide adequate temporary CPT facilities DoD OIG: (b)(7)(E)

~~(S//REL TO USA, FVEY)~~ ARMY; NAVY; USAF; USMC: (b)(1), Sec. 1.4(g)

(U) Management Actions Taken

~~(S//REL TO USA, FVEY)~~ ARMY; NAVY; USAF; USMC: (b)(1), Sec. 1.4(g)

~~(S//REL TO USA, FVEY)~~ ARMY; NAVY; USAF; USMC: (b)(1), Sec. 1.4(g)

(U) Recommendations

(U) We recommend that the Chiefs of Staff, U.S. Army and U.S. Air Force; the Chief of Naval Operations; the Commandant of the Marine Corps; and the Commander, USCYBERCOM:

- (U) develop or update a doctrine, organization, training, materiel, leadership and education, personnel, facilities, and policy framework to document capability requirements and associated capability gaps to build the current force, grow and mature the full CMF, and develop and sustain CMF capabilities, and



Results in Brief

(U//~~FOUO~~) Combat Mission Teams and Cyber Protection Teams Lacked Adequate Capabilities and Facilities to Perform Missions

- (U) formalize an agreement to focus capability development on functional and mission areas consistent with the results of the CMF mission alignment board to begin identifying capability gaps and developing capabilities that affected these proposed missions.

(U) We also recommend that the Commander, USCYBERCOM develop and specify the capability baseline and interoperability standards for CPTs. In addition, we recommend that the Commander, Army Cyber Command and Second Army develop a time-sensitive plan of actions and milestones to provide all Army CPTs with adequate workspace and consistent classified network access.

(U) Management Comments and Our Response

(U) We did not receive comments from the Chief of Staff for the Air Force and the Commandant of the Marine Corps in response to the draft report. Comments from the Chief of Naval Operations; Deputy Chief of Staff for the U.S. Army; and Commander, Army Cyber Command and Second Army, addressed the specifics of the recommendations. Comments from the Commander, USCYBERCOM, partially addressed the specifics of the recommendations, but further comments are required. We request management comment on the final report no later than December 24, 2015. Please see the Recommendations Table on the next page.

(U) Recommendations Table

Unclassified		
Management	Recommendations Requiring Comments	No Additional Comments Required
Chief of Staff, U.S. Army		1, 2
Chief of Naval Operations		1, 2
Chief of Staff, U.S. Air Force	1, 2	
Commandant of the Marine Corps	1, 2	
Commander, U.S. Cyber Command	1	2, 3
Commander, U.S. Army Cyber Command and Second Army		4
Unclassified		

(U) Please provide Management Comments no later than December 24, 2015.



~~SECRET//NOFORN~~

INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
4800 MARK CENTER DRIVE
ALEXANDRIA, VIRGINIA 22350-1500

November 24, 2015

(U) MEMORANDUM FOR DISTRIBUTION

(U//~~FOUO~~) SUBJECT: Combat Mission Teams and Cyber Protection Teams Lacked Adequate Capabilities and Facilities to Perform Missions
(Report No. DODIG-2016-026)

(U//~~FOUO~~) We are providing this final report for review and comment. U.S. Cyber Command, the Service Components, and the Defense Information Systems Agency made progress in providing Cyber Mission Force Teams with facilities, equipment, and capabilities to perform missions but did not take sufficient steps to ensure all teams had adequate capabilities and facilities. Specifically, U.S. Cyber Command, the Service Components, and the Defense Information Systems Agency lacked a unified approach to ensure Combat Mission Teams and Cyber Protection Teams had adequate capabilities to perform offensive and defensive missions. Additionally, Army Cyber Command did not provide select Army Cyber Protection Teams with adequate workspace or facilities to access needed networks. We conducted this audit in accordance with generally accepted government auditing standards.

(U) We considered management comments on a draft of this report when preparing the final report. However, the Chief of Staff for the U.S. Air Force and the Commandant of the Marine Corps did not comment on Recommendations 1 and 2. DoD Instruction 7650.03 requires that recommendations be resolved promptly. Therefore, we request the Chief of Staff and the Commandant provide comments on the recommendations no later than December 24, 2015.

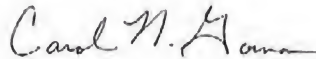
(U) Comments from the Commander, U.S. Cyber Command, addressed the specifics of Recommendation 2 and 3; however, the Commander partially addressed Recommendation 1. Comments from the Director, Warfare Integration, responding for the Chief of Naval Operations, and the Chief, Cyberspace and Information Operations Division, responding for the Chief of Staff for the U.S. Army, addressed the specifics of Recommendations 1 and 2. We request the Commander, U.S. Cyber Command, provide additional comments on the final report no later than December 24, 2015. Although not required to comment, the Commander, Marine Corps Forces Cyber Command and the Chief of Staff, Air Forces Cyber Command, generally agreed with the finding and recommendations.

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

(U) Please provide comments that conform to the requirements of DoD Instruction 7650.03. Classified comments must be sent electronically over the Secret Internet Protocol Router Network (SIPRNet). Please send a PDF file containing your comments to DoD OIG: (b)(6) @dodig.smil.mil and DoD OIG: (b)(6) @dodig.smil.mil. Copies of your comments must have the actual signature of the authorizing official for your organization. We cannot accept the /Signed/ symbol in place of the actual signature. Comments provided on the final report must be marked and portion-marked, as appropriate, in accordance with DoD Manual 5200.01. If you consider any matters to be exempt from public release, you should mark them clearly for Inspector General consideration.

(U) We appreciate the courtesies extended to the staff. Please direct questions to me at (703) 699-~~DO NOT DISSEMINATE~~ (DSN 499-~~DO NOT DISSEMINATE~~).



Carol N. Gorman
Assistant Inspector General
Readiness and Cyber Operations

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

(U) DISTRIBUTION:

(U) DEPUTY ASSISTANT SECRETARY OF DEFENSE FOR CYBER POLICY
(U) CHIEF OF STAFF, U.S. ARMY
(U) CHIEF OF NAVAL OPERATIONS
(U) CHIEF OF STAFF, U.S. AIR FORCE
(U) COMMANDANT OF THE MARINE CORPS
(U) COMMANDER, U.S. CYBER COMMAND
(U) COMMANDER, ARMY CYBER COMMAND AND SECOND ARMY
(U) COMMANDER, FLEET CYBER COMMAND AND 10TH FLEET
(U) COMMANDER, AIR FORCES CYBER COMMAND AND 24TH AIR FORCE
(U) COMMANDER, MARINE CORPS FORCES CYBER COMMAND
(U) DIRECTOR, JOINT STAFF
(U) DIRECTOR, DEFENSE INFORMATION SYSTEMS AGENCY

~~SECRET//NOFORN~~

(U) Contents

(U) Introduction

(U) Objective	1
(U) Background on DoD Cyberspace Operations	1
(U) CMF Development	2
(U) Cyberspace Responsibilities and Requirements	3
(U) Review of Internal Controls	6

(U//~~FOUO~~) Finding. Capabilities and Facilities for CMTs and CPTs Were Inadequate

(U) CMF Teams Had Adequate Desktop Equipment	8
(U) Unified Strategy and Approach for Offensive Capability Development Was Needed .	9
(U) DoD Lacked a Unified Defensive Capability Development Process	17
(U// FOUO) CMTs Faced Challenges in Performing Missions	22
(U// FOUO) Temporary Army CPT Facilities Provided Inadequate Workspace and Network Access	25
(U// FOUO) Inadequate Capabilities and Facilities Jeopardized CMF Mission Success	30
(U) Management Comments on the Finding and Our Response	31
(U) Recommendations, Management Comments, and Our Response	32
(U) Unsolicited Management Comments and Our Response	38

(U) Appendix

(U) Scope and Methodology	41
(U) Use of Computer-Processed Data	43
(U) Prior Coverage	44

(U) Management Comments

(U) U.S. Cyber Command	45
(U) Chief of Naval Operations	47
(U) U.S. Army Chief of Staff	50
(U) U.S. Army Cyber Command and Second Army	54
(U) U.S. Marine Corps Forces Cyber Command	55
(U) U.S. Air Forces Cyber Command and 24th Air Force	58

(U) Source of Classified Information

(U) Acronyms and Abbreviations

(U) Introduction

(U) Objective

(U) Our audit objective was to determine whether Cyber Mission Force (CMF) teams had adequate facilities, equipment, and capabilities¹ to effectively perform mission requirements. See Appendix A for the scope and methodology and prior audit coverage related to the objective.

(U) Background on DoD Cyberspace Operations

(U) DoD uses cyberspace to enable its military, intelligence, and business operations. Cyberspace is one of the five DoD domains; the other domains are air, land, maritime, and space. Cyberspace, unlike the other physical domains, is a global domain within the information environment that consists of interdependent networks of information technology infrastructures and resident data. Cyberspace operations ensure access and freedom of operations in, through, and from cyberspace to deliver effects² in any of the five domains; to deny adversaries access and freedom of operations; and to sustain mission essential segments of cyberspace (networks) in the face of adversary action. Cyberspace operations are categorized under three lines of operations, based on their intent:

1. (U//~~FOUO~~) **Offensive Cyberspace Operations.** Project power by the application of force in and through cyberspace.
2. (U//~~FOUO~~) **Defensive Cyberspace Operations.** Defend DoD or other friendly cyberspace.
3. (U//~~FOUO~~) **DoD Information Network (DoDIN) Operations.** Design, build, configure, secure, operate, maintain, and sustain DoD communications systems and networks.

¹ (U//~~FOUO~~) A cyber capability is a device, computer program, or technique—including any combination of software, firmware, and hardware—designed to create an effect in or through cyberspace.

² (U) Cyber effects include manipulating, disrupting, denying, degrading, or destroying information or communications systems, networks, physical or virtual infrastructure controlled by computers or information systems, or information resident on the infrastructure.

(U) CMF Development


~~(S//REL TO USA, FVEY)~~ ARMY; NAVY; USAF; USMC: (b)(1), Sec. 1.4(g)



~~(S//REL TO USA, FVEY)~~ Table 1. ARMY; NAVY; USAF; USMC: (b)(1), Sec. 1.4(g)

~~(S//REL TO USA, FVEY)~~

ARMY; NAVY; USAF; USMC: (b)(1), Sec. 1.4(g)



~~(S//REL TO USA, FVEY)~~

* (U) The Commander, Cyber National Mission Force, commands and controls National Mission Teams and National Support Teams to defend the nation in response to foreign hostile action or imminent threats in cyberspace.

³ (U) Figures presented in this report are rounded amounts.


~~(S//REL TO USA, FVEY)~~ ARMY; NAVY; USAF; USMC: (b)(1), Sec. 1.4(g)



~~(S//REL TO USA, FVEY)~~ Table 2. ARMY; NAVY; USAF; USMC: (b)(1), Sec. 1.4(g)

~~(S//REL TO USA, FVEY)~~

ARMY; NAVY; USAF; USMC: (b)(1), Sec. 1.4(g)



~~(S//REL TO USA, FVEY)~~

(U) Cyberspace Responsibilities and Requirements

(U) Under the authority of the Secretary of Defense, DoD uses cyberspace capabilities to perform integrated offensive and defensive operations. The Deputy Assistant Secretary of Defense for Cyber Policy, Office of the Under Secretary of Defense for Policy:

- (U) integrates cyberspace operations into national and DoD strategies;
- (U) develops policy related to cyber forces and employment of those forces; and
- (U) ensures cyber capabilities are integrated into operation and contingency plans.

⁴ (U) Additional information on the fielding of CMF teams is described in DoD OIG Report DODIG-2015-117, "USCYBERCOM and Military Services Need to Reassess Processes for Fielding CMF Teams," April 30, 2015 (S//NF).

(U) The Chairman of the Joint Chiefs of Staff ensures cyberspace plans and operations are compatible with other military plans. Although the Commander, U.S. Strategic Command is required to secure, operate, and defend the DoDIN and critical cyberspace assets, systems, and functions against an intrusion or attack, the Commander delegated most cyberspace responsibilities to the Commander, USCYBERCOM. The Commander, USCYBERCOM has three mission areas to counter threats to the DoDIN and military operations and to enable offensive cyberspace operations:

- (U) defend the Nation;
- (U) support Combatant Command contingency and operational planning; and
- (U) support the security, operation, and defense of the DoDIN.

(U) Additionally, USCYBERCOM:

- (U) develops a master implementation plan and schedule to accelerate the CMF build;
- (U) coordinates and prioritizes capability development across the Service Components and funds capabilities supporting joint requirements;
- (U) maintains the reliability of the cyber capabilities registry (CCR);⁵ and
- (S//REL TO USA, FVEY) ARMY; NAVY; USAF; USMC: (b)(1), Sec. 1.4(g)

⁵ (S//REL TO USA, FVEY) ARMY; NAVY; USAF; USMC: (b)(1), Sec. 1.4(g)

⁶ (S//REL TO USA, FVEY) ARMY; NAVY; USAF; USMC: (b)(1), Sec. 1.4(g)

- (U//~~FOUO~~) The other combatant commanders operate and defend their tactical and constructed networks and integrate cyberspace capabilities into all military operations. As such, combatant commanders are required to integrate cyberspace capabilities into their command plans and coordinate with other combatant commanders, the Service Components, and DoD agencies to create fully integrated capabilities.

(U) To support combatant commanders, Service Components staff, train, and equip forces and secure and defend their global networks. Additionally, the Service Components:

- (U) analyze missions and provide facilities for non-national CPTs;
- (U) coordinate with combatant commanders to locate combatant command CPTs;
- (U//~~FOUO~~) identify capability gaps and requirements through their Joint Force Headquarters-Cyber (JFHQ-C)⁷ and develop capabilities to support Service-specific and other joint capabilities when funded;
- (U) program, budget, maintain, and develop materiel solutions (for example, deployable toolkits) to meet CPT defensive capability needs; and
- (U) assist USCYBERCOM to determine CMF mission alignment.

(S//NF) ARMY; NAVY; USAF; USMC: (b)(1), Sec. 1.4(g)



⁷ (U//~~FOUO~~) The four JFHQ-C components (ARCYBER, FLTCYBER, AFCYBER, and MARFORCYBER) command and control the CMTs that conduct offensive operations in direct support of the combatant commands.

(U//~~FOUO~~) The Director, Defense Information Systems Agency (DISA), as the Commander, JFHQ-DoDIN, plans, directs, coordinates, integrates, and synchronizes the execution of missions that defend DoD networks. The Commander, JFHQ-DoDIN, develops agreements with Service Components to locate (provide facilities) and equip DoDIN CPTs.

(U) Review of Internal Controls

(U) DoD Instruction 5010.40, "Managers' Internal Control Program Procedures," May 30, 2013, requires DoD organizations to implement a comprehensive system of internal controls that provides reasonable assurance that programs are operating as intended and to evaluate the effectiveness of the controls. We identified internal controls weaknesses at USCYBERCOM. ARMY: (b)(7)(E)

[REDACTED]. We will provide a copy of the report to the senior officials responsible for internal controls at USCYBERCOM, ARCYBER, FLTCYBER, AFCYBER, and MARFORCYBER.

(U) Finding

(U//~~FOUO~~) Capabilities and Facilities for CMTs and CPTs Were Inadequate

(S//REL TO USA, FVEY) ARMY; NAVY; USAF; USMC: (b)(1), Sec. 1.4(g)

[REDACTED]

- (S//REL TO USA, FVEY) ARMY; NAVY; USAF; USMC: (b)(1), Sec. 1.4(g)
- [REDACTED]

- (S//REL TO USA, FVEY) ARMY; NAVY; USAF; USMC: (b)(1), Sec. 1.4(g)
- [REDACTED]

- (S//REL TO USA, FVEY) ARMY; NAVY; USAF; USMC: (b)(1), Sec. 1.4(g)
- [REDACTED]

- (U//~~FOUO~~) ARCYBER did not provide adequate temporary facilities⁸ DoD OIG: (b)(7)(E)
- [REDACTED]
- [REDACTED]
- [REDACTED]

⁸ (U//~~FOUO~~) Subject matter experts are responsible for tracking the progress of capability development throughout its lifecycle and completing operational testing and evaluation. USCYBERCOM refers to subject matter experts as tool champions.

~~(S//REL TO USA, FVEY)~~ ARMY; NAVY; USAF; USMC: (b)(1), Sec. 1.4(g)

(U) CMF Teams Had Adequate Desktop Equipment

(U//~~FOUO~~) USCYBERCOM, the Service Components, and DISA adequately equipped CMF teams with desktop equipment to perform administrative and mission requirements¹⁰ with the exception of ARCYBER CPTs located in ~~ARMY: (b)(7)(E)~~ ~~ARMY: (b)(7)(E)~~,¹¹ and a FLTCYBER CMT. USCYBERCOM, in coordination with the Service Components, developed desktop equipment baselines to support the Service Components and DISA in equipping the CMF teams. ~~ARMY: (b)(7)(E)~~ ~~ARMY: (b)(7)(E)~~

(U//~~FOUO~~) ~~ARMY: (b)(7)(E)~~

~~ARMY: (b)(7)(E)~~ See Appendix A for the teams visited. Although only AFCYBER developed a written implementation plan, ARCYBER, FLTCYBER, MARFORCYBER, and DISA established deliberate processes to equip CMF teams ~~ARMY: (b)(7)(E)~~. The Service Components and DISA either used the USCYBERCOM baseline to equip teams or equipped teams with similar desktop configurations based on established Component missions, internal collaboration with Service Component organizations, or a combination of the two approaches. In general, workstations included monitors and peripheral devices, classified and unclassified communication systems, and access to the Non-secure Internet Protocol Router

⁹ (U) An integrated approach is based on a Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel, Facilities, and Policy framework.

¹⁰ ~~(S//REL TO USA, FVEY)~~ ARMY; NAVY; USAF; USMC: (b)(1), Sec. 1.4(g)

¹¹ (U//~~FOUO~~) We discussed this issue further in the "Temporary Army CPT Facilities Provided Inadequate Workspace and Network Access" section of this report.

(S//NF) ARMY; NAVY; USAF; USMC; (b)(1), Sec. 1.4(g)

(U) Unified Strategy and Approach for Offensive Capability Development Was Needed

(U//~~FOUO~~) Service Components continued to use Component-specific approaches and strategies to develop offensive capabilities that aligned to traditional Component-specific mission areas rather than unify capability development to support the CMTs. This occurred because USCYBERCOM did not have appropriate authorities to effectively oversee and direct offensive capability development. Although USCYBERCOM developed the Cyber Force Concept of Operations and Employment¹² and Integrated Master Plan and Schedule and established the Integrated Capabilities Requirements Working Group and the CCR, these initiatives left gaps in unifying offensive capability development.

(U) The Government Accountability Office (GAO) reported that the Service Components used separate, service-specific approaches to identify and meet capability requirements.¹³ Consequently, GAO concluded that capabilities may vary across the Service Components. GAO recommended DoD develop and publish detailed policies and guidance that:

- (U) affect the categories of personnel who perform cyberspace operations;
- (U) support command and control relationships between USCYBERCOM and combatant commanders; and
- (U) address mission requirements and capabilities for the Service Components to meet to provide long-term operational support to USCYBERCOM.

(U) As of July 2015, two of the three recommendations were closed; the recommendation related to the categories of personnel remained open. Although GAO reported that the differences between the Components might be expected, it also

¹² (U) USCYBERCOM Cyber Force Concept of Operations and Employment, Version 4.1, July 22, 2014 (S//REL TO USA, FVEY).

¹³ (U) GAO-11-421, "More Detailed Guidance Needed to Ensure Military Services Develop Appropriate Cyberspace Capabilities," May 2011.


(U) questioned whether these differences were beneficial and whether the Service Components would be able to meet long-term capability requirements.

(U) Service-Specific Offensive Capability Development Processes Were Not Coordinated


(S//NF) ARMY; NAVY; USAF; USMC: (b)(1), Sec. 1.4(g)



(S//REL TO USA, FVEY) ARMY; NAVY; USAF; USMC: (b)(1), Sec. 1.4(g)




(S//REL TO USA, FVEY) ARMY; NAVY; USAF; USMC: (b)(1), Sec. 1.4(g)



¹⁴ (U) Concept of Operations for the JFHQ-C, Version 2.0, May 1, 2014 (S//REL TO USA, FVEY).

¹⁵ (S//REL TO USA, FVEY) ARMY; NAVY; USAF; USMC: (b)(1), Sec. 1.4(g)



¹⁶ (U) ARCYBER and Second Army Strategy for Defining Operational Requirements and Acquiring Capabilities, Version 2.2, October 22, 2012 (updated November 20, 2012) (S//NF).

~~(S//REL TO USA, FVEY)~~ ARMY; NAVY; USAF; USMC: (b)(1), Sec. 1.4(g)

~~(S//REL TO USA, FVEY)~~ ARMY; NAVY; USAF; USMC: (b)(1), Sec. 1.4(g)

(U) USCYBERCOM Actions Were Insufficient to Unify Capability Development

(U//~~FOUO~~) USCYBERCOM is the focal point for all DoD cyberspace operations. Specifically, USCYBERCOM:

- (U) identifies and prioritizes technical capability requirements;
- (U) monitors development of proposed technology solutions and architectural frameworks and associated interoperability standards;
- (U) oversees development of advanced tactics, techniques, and procedures to employ capabilities; and
- (U) oversees test and evaluation of cyberspace capabilities.

(U//~~FOUO~~) To meet its responsibilities, USCYBERCOM developed the Integrated Master Plan and Schedule, the Cyber Force Concept of Operations and Employment, established processes and the Integrated Capabilities Requirements Working Group to facilitate capability development, and created the CCR; however, these initiatives did not ensure a unified and coordinated approach to CMF capability development.

¹⁷ ~~(S//REL TO USA, FVEY)~~ ARMY; NAVY; USAF; USMC: (b)(1), Sec. 1.4(g)

(U) Cyber Capability Framework Was Lacking

(U) Although DoD was more than 2 years into the CMF build as of September 2015, the Components responsible for implementing the force did not have a comprehensive doctrine, organization, training, materiel, leadership and education, personnel, facilities, and policy (DOTMLPF-P) framework to guide CMF implementation. An integrated approach such as a DOTMLPF-P framework was needed to document capability requirements and associated capability gaps to build the current force, grow and mature the full CMF, and develop and sustain CMF capabilities. Guidance from many sources, including a DOTMLPF-P framework, influences military operations, intelligence activities, development and validation of capability requirements, acquisition activities affecting organization, training, and equipping forces, and the budget process to fund these activities.

(U) Components responsible for implementing the force did not have a comprehensive DOTMLPF-P framework.

(U) USCYBERCOM and the Joint Staff developed the Integrated Master Plan and Schedule to describe how DoD would implement the cyber force model through FY 2016. Although the Integrated Master Plan and Schedule primarily focused on staffing the CMF, it also recognized other critical aspects of building a force using a DOTMLPF-P framework, to include providing the CMF with capabilities to perform missions. However, USCYBERCOM did not develop a strategic roadmap for capability development. According to the Joint Staff, Command, Control, Communications and Computers (Cyber) Division, branch chief, the Integrated Master Plan and Schedule led to developing the Cyber Force Concept of Operations and Employment to continue addressing major cyberspace activities.

(U//~~FOUO~~) USCYBERCOM developed the Cyber Force Concept of Operations and Employment to describe fundamental principles and supporting tactics, techniques, and procedures to support the CMF in conducting military objectives. Although the Cyber Force Concept of Operations and Employment also provided planning guidance and described USCYBERCOM's way forward to build the CMF force model based on elements of a DOTMLPF-P framework, the analysis was not comprehensive and did not include planning facts, assumptions, and constraints that fully addressed known capability gaps that affected the CMF.

(U//~~FOUO~~) Furthermore, the Services did not develop a DOTMLPF-P framework that defined their strategies to build and field CMF teams. ARCYBER, FLTCYBER, AFCYBER, and MARFORCYBER officials acknowledged a strategic framework was needed; however, they stated that the Service Components were more concerned with staffing CMF teams than in establishing a DoD strategy involving full DOTMLPF-P consideration.

(U//~~FOUO~~) A MARFORCYBER official stated that the command took initiative to begin developing a DOTMLPF-P in 2013 to support its ability to implement the CMF for elements within its control; however, MARFORCYBER did not complete the framework because the command prioritized building and fielding CMF teams. Additionally, AFCYBER created a strategic plan, but did not complete a DOTMLPF-P framework.¹⁸

(U//~~FOUO~~) The cyber environment continues to rapidly evolve and is unconstrained by global boundaries that create unparalleled challenges to traditional military integration, synchronization, coordination, and deconfliction processes. These challenges, coupled with the tempo of cyberspace operations, require an approach that is more centralized and comprehensive to ensure the CMF is provided with needed and timely capabilities to perform missions. The lack of a joint USCYBERCOM-led DOTMLPF-P framework will continue to affect DoD's ability to implement an effective CMF. The Commander, USCYBERCOM; Chiefs of Staff for the U.S. Army and U.S. Air Force; the Chief of Naval Operations; and the Commandant of the Marine Corps, in coordination with the Commanders, ARCYBER, FLTCYBER, AFCYBER, and MARFORCYBER should develop a DOTMLPF-P framework to address strategies that build, grow, and sustain the CMF.

(U) Existing Cyber Capability Development Process Needed Improvement

(U//~~FOUO~~) USCYBERCOM's process defined in USCYBERCOM Instruction 3700-07¹⁹ to anticipate joint cyber warfighter requirements and develop solutions to meet these requirements was ineffective. The process included using the Integrated Capability Requirement Working Group and the CCR to provide situational awareness of DoD's offensive cyberspace development efforts. The process described how USCYBERCOM would prioritize, invest, and oversee operational requirements and cyberspace capabilities funded by the command. Although USCYBERCOM established these processes, USCYBERCOM officials stated that they did not have assurance that all

¹⁸ (C//REL TO USA, FVEY) ARMY; NAVY; USAF; USMC; (b)(1), Sec. 1.4(g)

¹⁹ (U) USCYBERCOM Instruction 3700-07, "Cyber Capability Development Policy" February 20, 2014, Section 2.1, "Cyberspace Capability Development Process."

(U//~~FOUO~~) Service Component cyber capability development efforts were vetted through the Integrated Capabilities Requirements Working Group or included in the CCR.

(U//~~FOUO~~) The Integrated Capabilities Requirements Working Group was established to assess capability gaps and synchronize, prioritize, and deconflict capability requirements and development. The Integrated Capability Requirements Working Group was intended to:

- (U//~~FOUO~~) review operational cyberspace requirements provided by the JFHQ-Cs for the Service Components, CMFs, combatant commands, and the JFHQ-DoDIN;
- (U//~~FOUO~~) assist in documenting operational, functional, and technical requirements; and
- (U//~~FOUO~~) recommend material and non-material solutions.

(U//~~FOUO~~) According to USCYBERCOM, the CCR was intended to improve information exchange, provide situational awareness of existing capabilities to reduce the risk of developing duplicative capabilities, and identify national offensive and defensive cyber capability gaps. However, the CCR was unreliable for providing situational awareness and did not support tool developers, operators, and planners because it only included developed capabilities. Specifically, officials from the Service Components responsible for capability development did not consider the CCR to be reliable because existing capabilities in the CCR did not fully describe the function or use of the capability and did not include capabilities under development. An extract from March 2015 showed incomplete or missing information and did not thoroughly describe the functions of the capabilities.²⁰ Without including all capabilities in the CCR and relevant information about each capability, the CCR was not effective and could not support developers and planners as intended.

(U//~~FOUO~~) The CCR was unreliable for providing situational awareness and did not support tool developers, operators, and planners because it only included developed capabilities.

²⁰ (U) We did not further describe the content of the CCR or identify the number and type of capabilities included in the database because the information is classified TOP SECRET.

(U) Actions Taken Improved the Reliability and Use of the CCR

(S//REL TO USA, FVEY) ARMY; NAVY; USAF; USMC: (b)(1), Sec. 1.4(g)



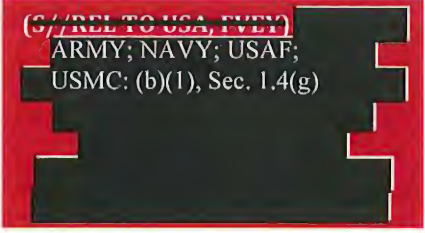
(U) Based on USCYBERCOM revisions to the CCR and its direction to include all offensive and defensive capabilities in the database, and the Deputy Secretary's required actions to make the CCR more reliable, we did not recommend further corrective actions.

(U) U.S. Cyber Command Lacked Authorities to Lead CMF Implementation, Development, and Sustainment

(S//REL TO USA, FVEY) ARMY; NAVY; USAF; USMC: (b)(1), Sec. 1.4(g)



(S//REL TO USA, FVEY)
ARMY; NAVY; USAF;
USMC: (b)(1), Sec. 1.4(g)



²¹ (U) USCYBERCOM Task Order 15-0087, "Directive to Enter or Update Cyber Capabilities into the CCR," Version 2.7, May 28, 2015 (U//FOUO).

²² (U) Deputy Secretary of Defense memorandum, "Follow-on Guidance from the April 18, 2015, Cyber Deep Dive," June 3, 2015 (S//REL TO USA, FVEY).

²³ (U) USCYBERCOM Operational Directive 12-001, April 5, 2012 (S//REL TO USA, FVEY).

(S//REL TO USA, FVEY) ARMY; NAVY; USAF; USMC: (b)(1), Sec. 1.4(g)



(S//REL TO USA, FVEY) ARMY; NAVY; USAF; USMC: (b)(1), Sec. 1.4(g)

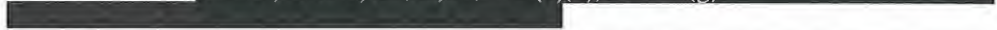


(U//~~FOUO~~) The Commanding General, ARCYBER, and the Second Army stated that resources, appropriate authorities, organizations, and capabilities, which could be synchronized in time and space with a singular purpose to accomplish directed missions, were needed.²⁵ In April 2015, USCYBERCOM, the Services, and DISA completed the “mission alignment board” to finalize proposed mission objectives for the remaining CMF teams to be fielded in FY 2015 and FY 2016. The outcome of the mission alignment board enabled USCYBERCOM and the Services to begin identifying capability gaps and developing capabilities that affected these proposed missions. However, USCYBERCOM officials acknowledged that the command lacked appropriate acquisition authorities and the ability to direct, when needed, Service capability development.

(U//~~FOUO~~) Resources, appropriate authorities, organizations, and capabilities, which could be synchronized in time and space with a singular purpose to accomplish directed missions, were needed

(U) The proposed National Defense Authorization Act for FY 2016 includes language to provide the Commander, USCYBERCOM limited acquisition authority to develop and acquire cyberspace-specific capabilities, equipment, and services. Proposed legislation recognizes the limitations of the USCYBERCOM Commander to ensure adequate capabilities are available to support CMF mission requirements; however, it does not

²⁴ (S//REL TO USA, FVEY) ARMY; NAVY; USAF; USMC: (b)(1), Sec. 1.4(g)



²⁵ (U) Statement by the Commanding General, ARCYBER and Second Army Before the House Armed Services Committee, Subcommittee on Emerging Threats and Capabilities, March 4, 2015.

(U) address other limitations that affect USCYBERCOM's ability to effectively oversee and, when needed, direct capability development.

(U//~~FOUO~~) Although the Commander's April 2012 Directive did not further unify Service cyber capability development because the Services did not agree with the approach, his goal was still valid based on the Services continued approach to independently develop capabilities that affected the CMF. The Commander, USCYBERCOM; the Chiefs of Staff for the U.S. Army and U.S. Air Force; the Chief of Naval Operations; and the Commandant of the Marine Corps should formalize an agreement to focus capability development on functional and mission areas consistent with results of the mission alignment board.

(U) DoD Lacked a Unified Defensive Capability Development Process

(U) The Service Components and DISA were independently developing Component-specific CPT toolkits²⁶ based on internal coordination, CPT personnel experience, and their individual interpretations of CPT capability needs. As of June 2015, the Service Components and DISA were not developing unified defensive capabilities.

(U) Service Component Efforts to Develop Defensive Capabilities

(S//REL TO USA, FVEY) ARMY; NAVY; USAF; USMC: (b)(1), Sec. 1.4(g)



(U//~~FOUO~~) The Army identified capabilities to include in the deployable toolkit through collaboration with a DISA CPT and ARCYBER and U.S. Army Network Enterprise

²⁶ (U//~~FOUO~~) A toolkit includes hardware and software that enables CPTs to conduct missions.

(U//~~FOUO~~) Technology Command interpretations of capabilities needed to perform defensive missions. ARMY: (b)(7)(E)

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

(S//REL TO USA, FVEY) ARMY; NAVY; USAF; USMC: (b)(1), Sec. 1.4(g)

[REDACTED]

- (U//~~FOUO~~) map specific operational environments;
- (U//~~FOUO~~) identify and prioritize potential security instances;
- (U//~~FOUO~~) perform hunt missions; and
- (U//~~FOUO~~) monitor a network or system.

(U//~~FOUO~~) As of March 2015, AFCYBER was modifying and providing additional capabilities to the Cyber Vulnerability Assessment-Hunter at an estimated cost of \$10.7 million to support CPTs.

(S//REL TO USA, FVEY) ARMY; NAVY; USAF; USMC: (b)(1), Sec. 1.4(g)

[REDACTED]

~~(S//REL TO USA, FVEY)~~ ARMY; NAVY; USAF; USMC: (b)(1), Sec. 1.4(g)



~~(S//REL TO USA, FVEY)~~ ARMY; NAVY; USAF; USMC: (b)(1), Sec. 1.4(g)



~~(S//REL TO USA, FVEY)~~ ARMY; NAVY; USAF; USMC: (b)(1), Sec. 1.4(g)



(U) DISA Efforts to Develop Defensive Capabilities

~~(S//REL TO USA, FVEY)~~ ARMY; DISA; NAVY; USAF; USMC: (b)(1), Sec. 1.4(g)



²⁷ (U) A rootkit is a collection of files installed on a system to alter the standard functionality of the system in a malicious and stealthy way.

(S//REL TO USA, FVEY) ARMY; DISA; NAVY; USAF; USMC: (b)(1), Sec. 1.4(g)



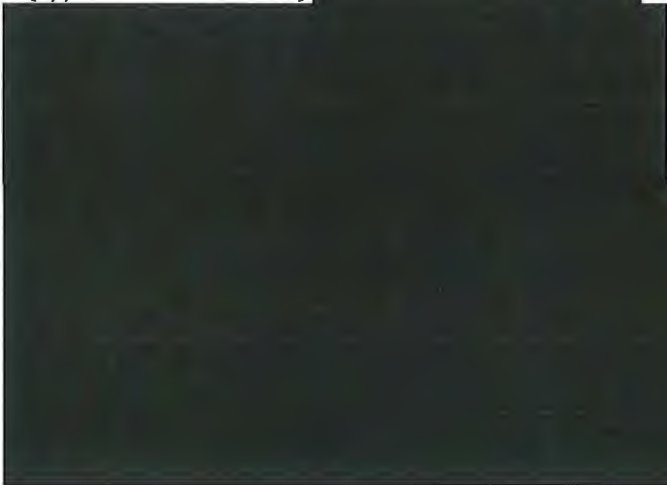
(S//REL TO USA, FVEY) ARMY; DISA; NAVY; USAF; USMC: (b)(1), Sec. 1.4(g)



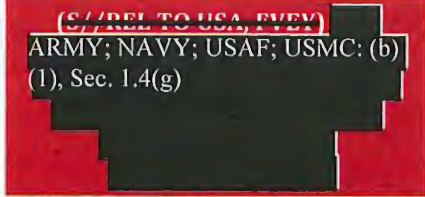
(U) CPT Capability Baseline Was Needed

(U//~~FOUO~~) The Service Components and DISA independently developed CPT toolkits based on their understanding of needed capabilities. This occurred because USCYBERCOM did not provide the Components guidance or standard CPT baseline requirements and interoperability standards to ensure each CPT could perform core defensive capabilities.

(S//REL TO USA, FVEY) ARMY; NAVY; USAF; USMC: (b)(1), Sec. 1.4(g)



(S//REL TO USA, FVEY)
ARMY; NAVY; USAF; USMC: (b)
(1), Sec. 1.4(g)



(U//~~FOUO~~) The FLTCYBER JFHQ-C Chief of Staff stated that different Components provided CPT support to DISA and the combatant commands. DoD OIG: (b)(7)(E)

[REDACTED]

(S//REL TO USA, FVEY) ARMY; NAVY; USAF; USMC: (b)(1), Sec. 1.4(g)

[REDACTED]

(U//~~FOUO~~) DoD OIG: (b)(7)(E)

[REDACTED]

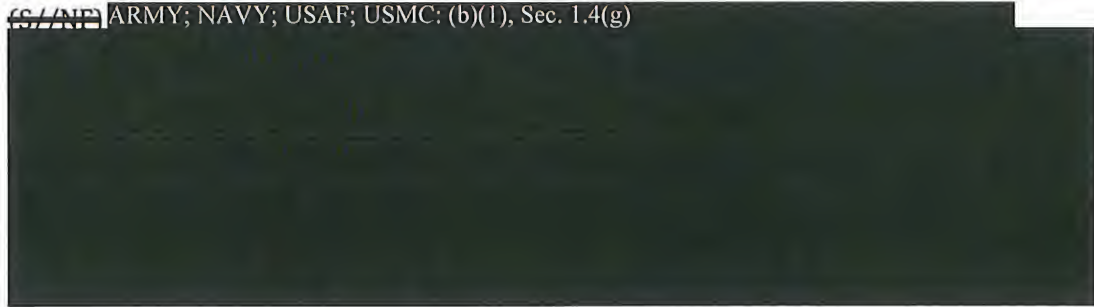
(U//~~FOUO~~) USCYBERCOM officials stated that they planned to use the recommended requirements to develop a baseline for all CPTs by October 2015. Although USCYBERCOM initiated steps to provide a CPT baseline, the baseline was not approved or developed. DoD OIG: (b)(7)(E)

[REDACTED]

[REDACTED] The Commander, USCYBERCOM, in coordination with the Service Components and DISA, should develop and specify a capability baseline and interoperability standards for CPTs.

(U//~~FOUO~~) CMTs Faced Challenges in Performing Missions

(S//NF) ARMY; NAVY; USAF; USMC: (b)(1), Sec. 1.4(g)

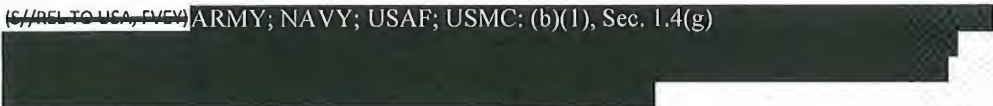


- (U) cyberspace intelligence, surveillance, and reconnaissance;
- (U) operational preparation of the environment;²⁹
- (U) defensive cyberspace operations – response actions;³⁰ and
- (U) offensive cyberspace operations.

(S//NF) ARMY; NAVY; USAF; USMC: (b)(1), Sec. 1.4(g)



²⁸ (S//REL TO USA, FVEY) ARMY; NAVY; USAF; USMC: (b)(1), Sec. 1.4(g)



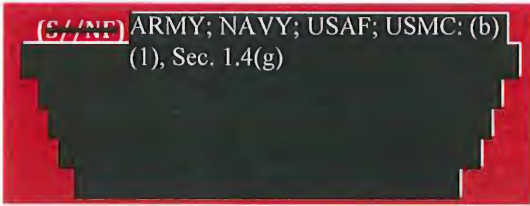
²⁹ (U) Operational preparation of the environment includes activities in likely or potential areas of operations to prepare and shape the operational environment.

³⁰ (U) Defensive cyberspace operations-response actions are deliberate, authorized defensive measures or activities taken outside of the defended network to protect and defend DoD cyberspace capabilities or designated systems.

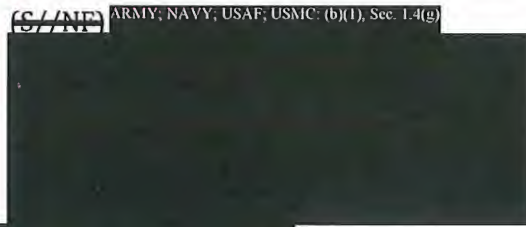
³¹ (U) Section 403-5, title 50, United States Code (2011) authorizes intelligence activities in response to national intelligence requirements.

(U) Finding

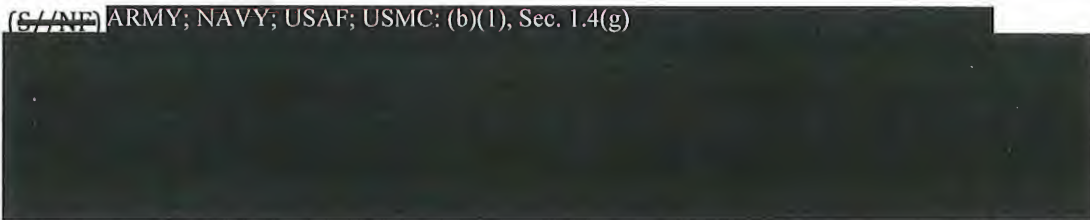
(S//NF) ARMY; NAVY; USAF; USMC: (b)(1), Sec. 1.4(g)



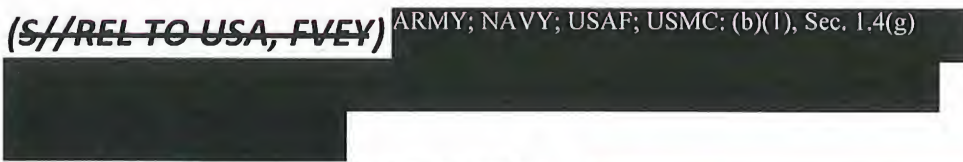
(S//NF) ARMY; NAVY; USAF; USMC: (b)(1), Sec. 1.4(g)



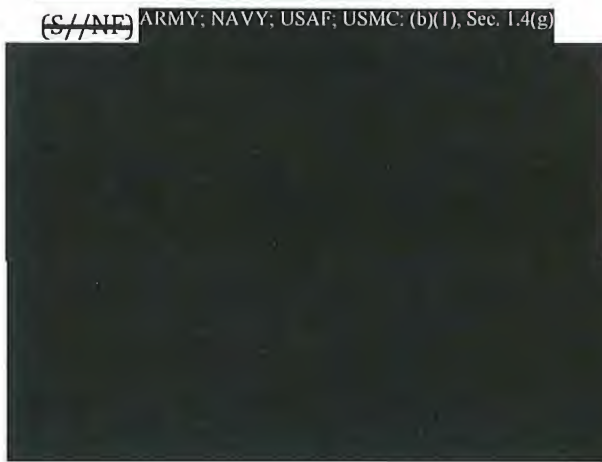
(S//NF) ARMY; NAVY; USAF; USMC: (b)(1), Sec. 1.4(g)



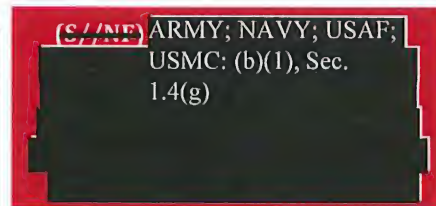
(S//REL TO USA, FVEY) ARMY; NAVY; USAF; USMC: (b)(1), Sec. 1.4(g)



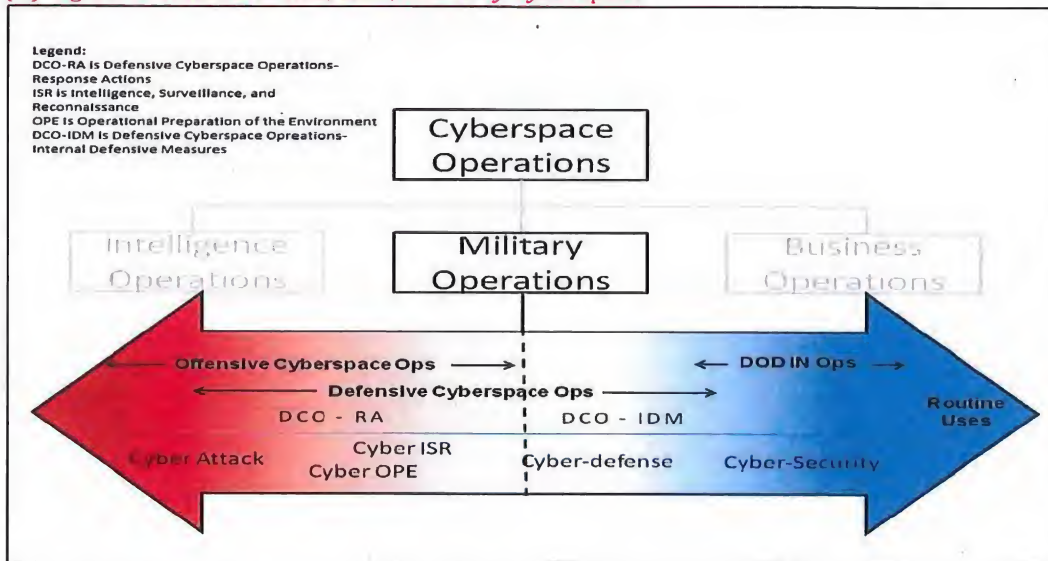
(S//NF) ARMY; NAVY; USAF; USMC: (b)(1), Sec. 1.4(g)



(S//NF) ARMY; NAVY; USAF; USMC: (b)(1), Sec. 1.4(g)



(U) Figure 1. Actions in Red, Blue, and Grey Cyberspace




(U) Source: USCYBERCOM Cyber Force Concept of Operations and Employment

(S//NF) ARMY; NAVY; USAF; USMC: (b)(1), Sec. 1.4(g)

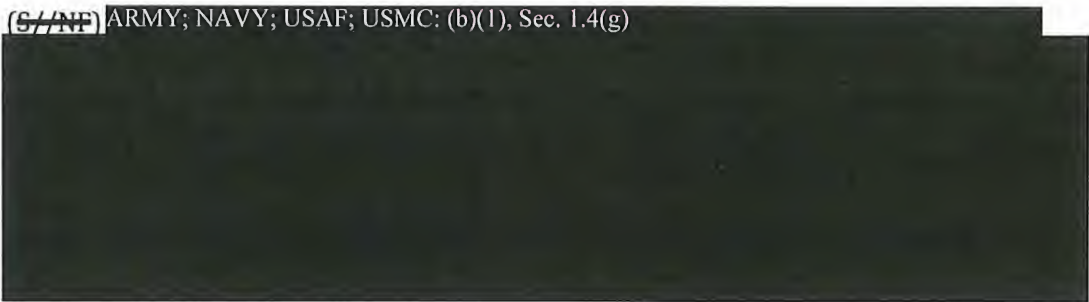
(S//NF) ARMY; NAVY; USAF; USMC: (b)(1), Sec. 1.4(g)

(S//NF) ARMY; NAVY; STRATCOM; USAF; USMC: (b)(1), Sec. 1.4(g)

(S//NF) ARMY; NAVY; USAF; USMC: (b)(1), Sec. 1.4(g)



(S//NF) ARMY; NAVY; USAF; USMC: (b)(1), Sec. 1.4(g)

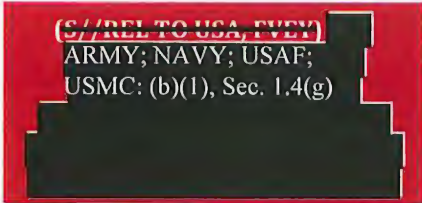


(U//~~FOUO~~) Temporary Army CPT Facilities Provided Inadequate Workspace and Network Access

(S//REL TO USA, FVEY) ARMY; NAVY; USAF; USMC: (b)(1), Sec. 1.4(g)



(S//REL TO USA, FVEY)
ARMY; NAVY; USAF;
USMC: (b)(1), Sec. 1.4(g)



³² (U) Sections 111, 164, and 167, title 10, United States Code, establish authorities and responsibilities for the Services and combatant commands to conduct military operations, including offensive cyberspace operations.

³³ (S) ARMY; NAVY; USAF; USMC: (b)(1), Sec. 1.4(g)



³⁴ (U) USCYBERCOM Cyber Force Concept of Operations and Employment, version 4.1, July 22, 2014 (S//REL TO USA, FVEY).

~~(S//REL TO USA, FVEY)~~ ARMY; NAVY; USAF; USMC: (b)(1), Sec. 1.4(g)



(U//~~FOUO~~) ARMY: (b)(7)(E)



(U//~~FOUO~~) ARMY: (b)(7)(E)



(U//~~FOUO~~) ARMY: (b)(7)(E)



(U//~~FOUO~~) ARMY: (b)(7)(E)



³⁵ (U//~~FOUO~~) ARMY: (b)(7)(E)



³⁶ (U) The Cyber Protection Brigade is subordinate to the 7th Signal Command.

³⁷ (U) The 513th Military Intelligence Brigade is a subordinate command to the U.S. Army Intelligence and Security Command.

(U//~~FOUO~~) ARMY: (b)(7)(E)


A large rectangular area of text is completely redacted with black bars.

(U//~~FOUO~~) ARMY: (b)(7)(E)

A large rectangular area of text is completely redacted with black bars.

(U) See Table 3 on the next page for the locations of ARCYBER temporary CPT facilities

ARMY: (b)(7)(E)

A rectangular area of text is completely redacted with black bars.

~~(S//REL TO USA, FVEY)~~ Table 3. ARMY; NAVY; USAF; USMC: (b)(1), Sec. 1.4(g)

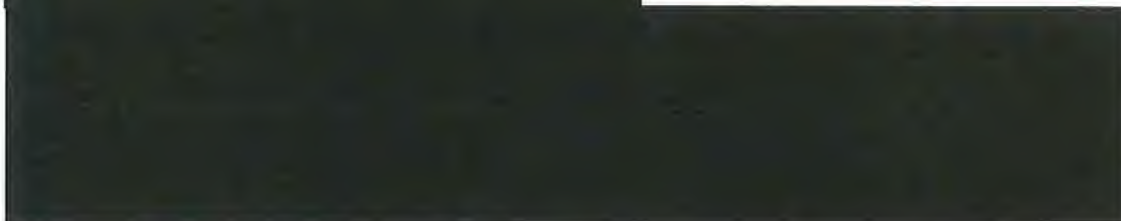
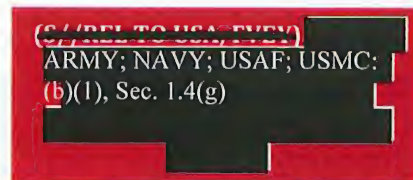
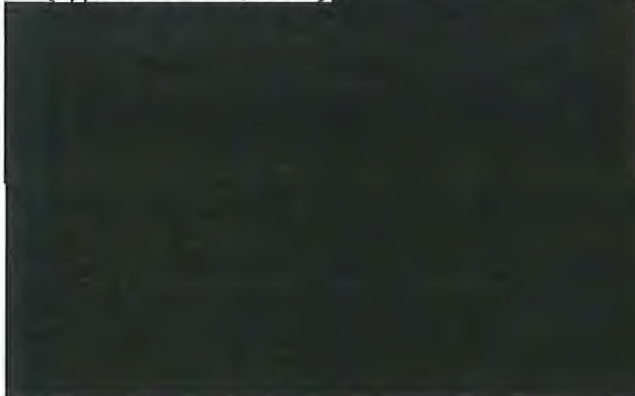
~~(S//REL TO USA, FVEY)~~

ARMY; NAVY; USAF; USMC: (b)(1), Sec. 1.4(g)

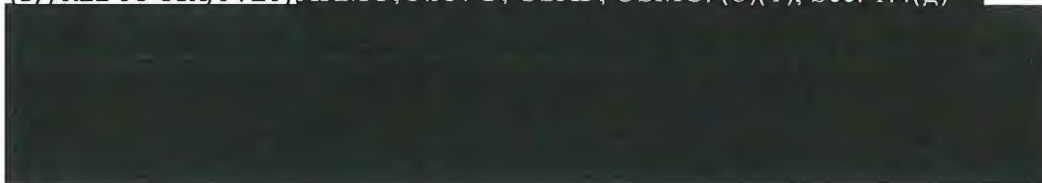


~~(S//REL TO USA, FVEY)~~

~~(S//REL TO USA, FVEY)~~ ARMY; NAVY; USAF; USMC: (b)(1), Sec. 1.4(g)



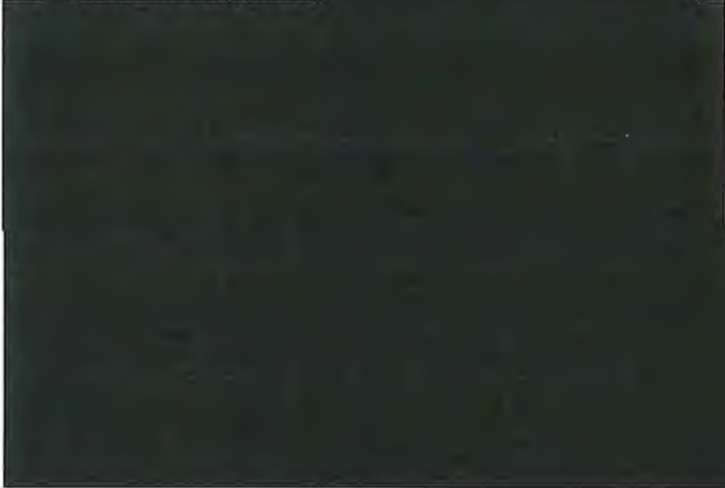
~~(S//REL TO USA, FVEY)~~ ARMY; NAVY; USAF; USMC: (b)(1), Sec. 1.4(g)



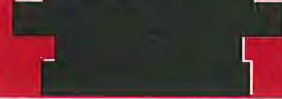
(S//REL TO USA, FVEY) ARMY; NAVY; USAF; USMC: (b)(1), Sec. 1.4(g)



(S//REL TO USA, FVEY) ARMY; NAVY; USAF; USMC: (b)(1), Sec. 1.4(g)



(S//REL TO USA, FVEY)
ARMY; NAVY;
USAF; USMC: (b)(1),
Sec. 1.4(g)



(S//REL TO USA, FVEY) ARMY; NAVY; USAF; USMC: (b)(1), Sec. 1.4(g)



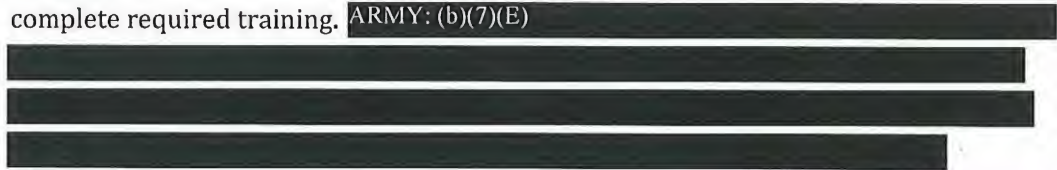
³⁸ (U) Cyber key terrain is any physical or logical elements of a domain that enable mission-essential warfighting functions.

(U//~~FOUO~~) Inadequate Capabilities and Facilities Jeopardized CMF Mission Success

(S//REL TO USA, FVEY) ARMY; NAVY; USAF; USMC: (b)(1), Sec. 1.4(g)



(U//~~FOUO~~) The Service Components were responsible for providing adequate facilities for non-national CPTs; however, ARCYBER temporary solutions did not provide up to ARMY: (b)(7)(E) with adequate workspace and network access to perform missions and complete required training. ARMY: (b)(7)(E)



(U) To continue to progress in cyberspace operations, DoD needs to close the capability gaps we identified and provide CMF teams with appropriate and adequate capabilities, facilities, and network access to maintain its warfighting advantage. A cyber force, when resourced with the appropriate infrastructure, platforms, and tools, is the key to dominance in cyberspace.

(U) To continue to progress in cyberspace operations, DoD needs to close the capability gaps we identified and provide CMF teams with appropriate and adequate capabilities, facilities, and network access to maintain its warfighting advantage.

(U) Management Comments on the Finding and Our Response

(U) Chief of Staff for the U.S. Army Comments

~~(S//REL TO USA, FVEY)~~ ARMY; USAF; USMC: (b)(1), Sec. 1.4(g)



(U) Our Response

(U//~~FOUO~~) We commend the Army for starting the study to identify funding to restore and modernize existing facilities. We recognize and did not intend to imply that the Army did not use a deliberate decision-making process ~~ARMY: (b)(7)(E)~~
~~ARMY: (b)(7)(E)~~. Although we asked on several occasions whether the Army conducted assessments ~~ARMY: (b)(7)(E)~~
~~we were not provided the cost-benefit analysis.~~

~~(S//REL TO USA, FVEY)~~ ARMY; USAF; USMC: (b)(1), Sec. 1.4(g)



(U//~~FOUO~~) As previously reported, the Army did not conduct a detailed assessment to conclude whether ~~ARMY: (b)(7)(E)~~ had sufficient SCIF workspace until August 2013. Therefore, we did not revise the report based on the additional documentation provided by the Army.

(U) Recommendations, Management Comments, and Our Response

(U) Recommendation 1

(U) We recommend the Commander, U.S. Cyber Command, and the Chiefs of Staff for the U.S. Army and U.S. Air Force, the Chief of Naval Operations, and the Commandant of the Marine Corps develop a doctrine, organization, training, materiel, leadership and education, personnel, facilities, and policy framework that address strategies to build, grow, and sustain the Cyber Mission Force.

(U) Commander, U.S. Cyber Command Comments

(S//NF) ~~ARMY; USAF; USMC: (b)(1), Sec. 1.4(g)~~



(U) Our Response

(U) Comments from the Commander partially addressed the recommendation. Although the Commander agreed with the recommendation to build and mature its existing DOTMLPF-P framework, he did not state the specific actions USCYBERCOM would take to provide a comprehensive strategy across all elements of the DOTMLPF-P framework. Therefore, we request that the Commander, USCYBERCOM, provide comments on the final report no later than December 24, 2015.

(U) Chief of Naval Operations Comments

(U//~~FOUO~~) The Director, Warfare Integration, responding for the Chief of Naval Operations, ~~NAVY: (b)(5)~~

~~[REDACTED]~~
~~[REDACTED]~~
~~[REDACTED]~~
~~[REDACTED]~~
~~[REDACTED]~~
~~[REDACTED]~~
~~[REDACTED]~~
~~[REDACTED]~~
~~[REDACTED]~~
~~[REDACTED]~~

(U) Our Response

(U) Comments from the Director addressed the recommendation, and no further comments are required.

(U) Chief of Staff for the U.S. Army Comments

(U//~~FOUO~~) The Chief, Cyberspace and Information Operations Division, responding for the Chief of Staff for the U.S. Army, agreed, stating that the Army was in the process of developing a comprehensive cyberspace strategy that presented the Army's vision to have cyberspace operational forces, capabilities, facilities, and partnerships ready and able to effectively provide support to regional, global, joint, and Army operations. The Chief stated that the strategy would drive investment, workforce, facility, and doctrinal changes. Additionally, the Chief stated that the U.S. Army Training and Doctrine Command established a Cyber Center of Excellence in January 2014 to serve as the Army's lead organization for Force Modernization. Since the Cyber Center of Excellence was established, the Chief stated it developed a DOTMLPF-P framework and a strategy to build, grow, and sustain soldiers under a new Career Management Field (CMF-17) to meet Army CMF requirements.

(U//~~FOUO~~) However, the Chief stated a need also existed for a Joint Services assessment across the entire DOTMLPF-P that focused on integrating efforts and strategies to further support building, growing, and sustaining the CMF. Specifically, the

(U//~~FOUO~~) Chief stated that a Joint Services assessment would allow the Services to share independent strategies, identify cross-cutting capabilities, and foster innovative approaches.

(U) Our Response

(U//~~FOUO~~) Comments from the Chief addressed the recommendation, and no further comments are required. We agree an overarching, Joint Services DOTMLPF-P assessment is needed and would benefit DoD's ability to build, grow, and sustain the CMF. Our intent was for USCYBERCOM, as the DoD cyberspace focal point, to lead efforts to develop a comprehensive DOTMLPF-P framework based on its assessment and the individual assessments and strategies developed by the Service Components.

(U) Management Comments Required

(U) The Chief of Staff for the U.S. Air Force and the Commandant of the Marine Corps did not respond to the recommendation. The Chief of Staff, AFCYBER, provided comments on the draft report; however, Air Force officials stated that comments from the Chief of Staff for the U.S. Air Force would be provided only in response to the final report. The Commander, MARFORCYBER, also provided comments on the draft report, but documentation from Headquarters, Marine Corps clearly stated that the comments represented MARFORCYBER's position. Although we attempted to clarify whether MARFORCYBER was responding on behalf of the Commandant, we did not receive a further response from the Marine Corps. We request the Chief of Staff for the U.S. Air Force and the Commandant of the Marine Corps provide comments on the final report no later than December 24, 2015.

(U) Recommendation 2

(U) We recommend the Commander, U.S. Cyber Command, and the Chiefs of Staff for the U.S. Army and U.S. Air Force, the Chief of Naval Operations, and the Commandant of the Marine Corps formalize an agreement to focus capability development on functional and mission areas consistent with results of the mission alignment board.

(U) Commander, USCYBERCOM Comments

(U//~~FOUO~~) The Commander, USCYBERCOM, agreed, stating that it was important for the cyber force to have an integrated approach for capability development. The

(U//~~FOUO~~) Commander stated that USCYBERCOM needed to engage with the Office of Secretary of Defense and Service Chiefs to coordinate and begin developing formal agreements to focus capability development and facilitate integrated development approaches. The Commander also stated that limited acquisition authority described in the draft FY 2016 National Defense Authorization Act, if received, would support increased capability development of functional and mission areas consistent with the results of the mission alignment board.

(U) Our Response

(U) Comments from the Commander addressed the recommendation, and no further comments are required.

(U) Chief of Naval Operations Comments

(S//REL TO USA, FVEY) ARMY; NAVY; USAF; USMC; (b)(1), Sec. 1.4(g)




(U) Our Response

(U) Comments from the Director addressed the recommendation, and no further comments are required.

(U) Chief of Staff for the U.S. Army Comments

(U//~~FOUO~~) The Chief, Cyberspace and Information Operations Division, responding for the Chief of Staff for the U.S. Army, agreed, stating that a formal memorandum of understanding for capability development that focused on the CMF mission alignment board for CMTs and CPTs was needed between the Services. The Chief stated that the Army's recently established Cyber Acquisition, Requirements, and Resourcing working group shaped the Army's efforts by providing requirements and acquisition support needed to rapidly develop and deliver new Army cyberspace capabilities to its force.

ARMY; (b)(7)(E)



(U//FOUO) ARMY: (b)(7)(E)



(U) Our Response

(U) Comments from the Chief addressed the recommendation, and no further comments are required.

(U) Management Comments Required

(U) The Chief of Staff for the U.S. Air Force and the Commandant of the Marine Corps did not respond to the recommendation. The Chief of Staff, AFCYBER, provided comments on the draft report; however, Air Force officials stated that comments from the Chief of Staff for the U.S. Air Force would be provided only in response to the final report. The Commander, MARFORCYBER, also provided comments on the draft report, but documentation from Headquarters, Marine Corps clearly stated that the comments represented MARFORCYBER's position. Although we attempted to clarify whether MARFORCYBER was responding on behalf of the Commandant, we did not receive a further response from the Marine Corps. We request the Chief of Staff for the U.S. Air Force and the Commandant of the Marine Corps provide comments on the final report no later than December 24, 2015.

(U) Recommendation 3

(U) We recommend that the Commander, U.S. Cyber Command, in coordination with the Service Components and the Defense Information Systems Agency, develop and specify a capability baseline and interoperability standards for all Cyber Protection Teams.

(U) Commander, USCYBERCOM Comments

(S//REL TO USA, FVEY) ARMY; USAF; USMC: (b)(1), Sec. 1.4(g)



~~(S//REL TO USA, FVEY)~~ ARMY; USAF; USMC: (b)(1), Sec. 1.4(g)

(U) Our Response

(U) Comments from the Commander addressed the recommendation, and no further comments are required.

(U) Chief of Naval Operations Comments

~~(S//REL TO USA, FVEY)~~ ARMY; NAVY; USAF; USMC: (b)(1), Sec. 1.4(g)

(U) Our Response

~~(S//REL TO USA, FVEY)~~ ARMY; USAF; USMC: (b)(1), Sec. 1.4(g)

(U) Recommendation 4

(U) We recommend the Commander, Army Cyber Command and Second Army develop a time-sensitive plan of action and milestones to provide all Army Cyber Protection Teams with adequate workspace ARMY: (b)(7)(E)

(U) Commander, U.S. Army Cyber Command and Second Army Comments

(U) The Commander, ARCYBER, agreed, stating that the U.S. Army Network Enterprise Technology Command was working with the Cyber Protection Brigade to assist in resourcing facilities and network improvements. The Commander stated that ARCYBER and the U.S. Army Network Enterprise Technology Command completed a full facility

(U) and network analysis of capabilities needed and developed a plan of action and milestones to provide Army CPTs with adequate workspace ARMY: (b)(7)(E)

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

(U) Our Response

(U) Comments from the Commander addressed the recommendation, and no further comments are required.

(U) Unsolicited Management Comments and Our Response

(U) Commander, MARFORCYBER Comments

~~(S//REL TO USA, FVEY)~~ ARMY; USAF; USMC: (b)(1), Sec. 1.4(g)

[REDACTED]

(U//~~FOUO~~) Additionally, the Commander stated that a formal capability development agreement was not needed. Instead, the Commander stated that the issuance of a task order, operational order, or fragmentary order would be more appropriate. The Commander noted that the mission alignment board process was relevant to only CMTs and NMTs, not CPTs. Further, the Commander stated that a capability baseline and interoperability standard for CPTs was needed. However, the Commander noted that the baseline should not restrict CPTs from adapting their tools and methodologies to meet emerging threats. The Commander stated that the baseline should be established using functional and mission analysis of CPT operations that considered the current

(U//~~FOUO~~) operating environment as well as the expected future Joint Information Environment. The Commander stated that an acceptable tools list with a universal authority to operate on the DoDIN, or portions of the DoDIN, was also needed to provide CPTs with flexible options to enable them to rapidly implement and respond to incidents.

(U) Our Response

(U//~~FOUO~~) We commend MARFORCYBER for developing a strategy to incrementally complete a MARFORCYBER-wide DOTMLPF-P framework to build, grow, and sustain the CMF and for recently completing its first assessment as part of the strategy. MARFORCYBER recognized that the CPT baseline capability should be based on functional and mission analysis and be approved to operate on the DoDIN or portions of it to increase the CPTs' ability to promptly and effectively perform incident response missions. We acknowledge that the CPT capability baseline should not restrict CPTs from adapting their tools and methodology to meet emerging threats.

(U//~~FOUO~~) We recognize and agree that capability development to support the CMF should be a joint effort. We understand other types of written direction could meet our intent. However, as stated in this report, similar efforts by the Commander, USCYBERCOM, to specifically direct capability development efforts in Operational Directive 12-001 were not successful because agreement between the Services and USCYBERCOM had not been reached. As the Services and DoD continue to develop a broad range of cyberspace tools and capabilities, an agreement and collaboration among the Services and USCYBERCOM to align multiple capability development efforts and reduce potential redundancy while meeting combatant command and Service requirements is needed. The lack of broader agreement to synchronize and leverage Service-led capability development efforts could result in developing redundant capabilities and, therefore, not using limited resources efficiently.

(U) AFCYBER and 24th Air Force Comments

(U//~~FOUO~~) Although not required to comment, the Chief of Staff, AFCYBER, stated that AFCYBER would continue to work with Headquarters, U.S. Air Force and USCYBERCOM to develop or update a DOTMLPF-P framework. The Chief of Staff stated that AFCYBER would also continue to document capability requirements and associated capability gaps to build the current force, grow and mature the full CMF, and develop and sustain CMF capabilities. However, the Chief of Staff stated that an Air Force Space Command

(U//~~FOUO~~) Project Task Force already made progress towards institutionalizing a DOTMLPF-P framework and developed a strategic level doctrinal framework in the CMF Program Action Directive, January 15, 2014.

(U//~~FOUO~~) The Chief of Staff stated that the CMF Program Action Directive established DOTMLPF-P guidance that included planning actions focused on training, budget, facilities, equipment, and personnel across the total force for the Air Force CMF build. The Chief of Staff stated that the framework supported the Air Force in building

DoD OIG: (b)(7)(E)

DoD OIG: (b)(7)(E). The Chief of Staff also stated that the current strategic guidance enabled AFCYBER to successfully field, train, organize, equip, and develop capabilities to meet Air Force CMF needs across the entire Air Force presentation of forces.

(U//~~FOUO~~) Additionally, the Chief of Staff stated AFCYBER would continue to work with Headquarters, U.S. Air Force, USCYBERCOM, and other CMF oversight organizations, in accordance with the Cyber Force Concept of Operations and Employment, to formalize agreements that allow combatant commanders to direct capability development that supports their mission requirements and priorities.

(U) Our Response

(U) We commend AFCYBER for developing a strategic roadmap to build, grow, and sustain the CMF. We recognize the Air Force Space Command strategy provides the foundation for AFCYBER to develop and update its DOTMLPF-P framework. Additionally, we commend AFCYBER for acknowledging the need existed to formalize agreements to develop capabilities that support Service and combatant commander mission requirements and priorities.

(U) Appendix

(U) Scope and Methodology

(U) We conducted this performance audit from November 2014 through September 2015 in accordance with Generally Accepted Government Auditing Standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

(U) We visited Headquarters, USCYBERCOM, and Headquarters, NSA, Fort Meade, Maryland. Specifically, we interviewed officials from the USCYBERCOM Operations Directorate (J3), Logistics Directorate (J4), Capability and Resource Integration Directorate (J8), and Advanced Concepts and Technology Directorate (J9) to determine their processes for identifying requirements, developing implementation plans and strategies to locate CMF teams in appropriate workspaces with access to needed networks, and planning and funding facilities, equipment, and capabilities to support CMF teams.

(U//~~FOUO~~) We also interviewed USCYBERCOM officials to determine processes for coordinating and facilitating capability development across the Service Components. Additionally, we met with the Commander, Cyber National Mission Force, to discuss his vision for pooling CMF tool developers, assigning CMF missions and targets, and standardizing CPT requirements and capabilities. Further, we attended the [REDACTED] DoD OIG: (b)(7)(E) exercise to observe the types of capabilities a NMT and national CPT used or had access to for performing missions.

(U//~~FOUO~~) NSA: (b)(3), 10 USC § 3605
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

(U//~~FOUO~~) We reviewed three task and two fragmentary orders issued by USCYBERCOM and the implementation plan for fielding the CMF teams; standard equipment configurations based on CMF team work roles to identify desktop equipment

(U//~~FOUO~~) NSA: (b)(3), 10 USC § 3605

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

(U//~~FOUO~~) We visited Headquarters, ARCYBER, Fort Meade, Maryland; Headquarters, FLTCYBER, Fort Meade, Maryland; Headquarters, AFCYBER, Joint Base San Antonio-Lackland, Texas; and Headquarters, MARFORCYBER, Columbia, Maryland. We interviewed officials from ARCYBER, FLTCYBER, AFCYBER, and MARFORCYBER responsible for staffing, equipping, assessing locations and providing facilities, and identifying capability gaps and developing capabilities to support Service-fielded CMF teams. Additionally, we interviewed officials from ARCYBER, FLTCYBER, AFCYBER, and MARFORCYBER to identify responsibilities for providing administrative and operational control of the CMF. We reviewed agreements to identify facilities and responsibilities for locating Army, Navy, and Marine Corps CMF teams; ARCYBER, AFCYBER, and FLTCYBER assessments to identify processes and criteria for locating CMF teams; plans for locating CMF teams to identify temporary and permanent CPT facilities; initial and full operational capability designations to identify the missions of CMF teams; and operational needs, capability gaps, and CPT flyaway kit configurations to identify offensive and defensive capabilities used or needed by CMTs and CPTs.

(U) In addition, we interviewed officials from Joint Staff Operations Directorate (J3), Command, Control, Communications and Computer Directorate (J6), Joint Force Development Directorate (J7), and Force Structure, Resource and Assessment Directorate (J8) to determine oversight responsibilities for implementing the CMF build and to identify their involvement in identifying CMF facility, equipment, and capability requirements. We also interviewed officials from the U.S. Pacific Command and U.S. European Command joint cyber centers responsible for developing missions and targets, integrating cyberspace into command plans and operations, and coordinating facility and capability gaps with their respective JFHQ-Cs. We reviewed integrated priority lists identifying cyberspace priorities and capability gaps; mission and target assignments for CMTs; and unfunded CPT facility requirements.

(U) NSA: (b)(3), 10 USC § 3605

Component-designated facilities; and Headquarters, DISA, Fort Meade, Maryland. We interviewed CMF team leads, deputy team leads, and non-commissioned officers in charge responsible for assessing equipment and capability needs and planning, implementing, and leading team missions to review the adequacy of their facilities, equipment, and capabilities. See Table A.1 for the Service Component that fielded the teams, the specific CMF team visited, and the location of each team.

~~(S//REL TO USA, FVEY)~~ Table A.1.

ARMY; NAVY; USAF; USMC: (b)(1), Sec. 1.4(g)

~~(S//REL TO USA, FVEY)~~

ARMY; NAVY; USAF; USMC: (b)(1), Sec. 1.4(g)

~~(S//REL TO USA, FVEY)~~

(U) We also reviewed USCYBERCOM, NSA Central Security Service, U.S. Pacific Command, and U.S. European Command security classification guides to appropriately classify information and portion mark the report.

(U) Use of Computer-Processed Data

(U) We did not use computer-processed data to perform this audit.

(U) Prior Coverage

(U) During the last 5 years, the GAO and the Department of Defense Inspector General (DoD IG) issued six reports discussing DoD's ability to resource and conduct cyberspace operations. Unrestricted GAO reports can be accessed over the Internet at <http://www.gao.gov>.

(U) GAO

(S) ARMY; USAF; USMC: (b)(1), Sec. 1.4(g)

(U) Report No. GAO-11-75, "Defense Department Cyber Efforts: DoD Faces Challenges in its Cyber Activities," July 25, 2011

(U) Report No. GAO-11-421, "Defense Department Cyber Efforts: More Detailed Guidance Needed to Ensure Military Services Develop Appropriate Cyberspace Capabilities," May 20, 2011

(S) ARMY; USAF; USMC: (b)(1), Sec. 1.4(g)

(U) DoD OIG

(U) Report No. DODIG-2015-117, "USCYBERCOM and Military Services Need to Reassess Processes for Fielding CMF Teams," April 30, 2015 (S//NF)

(U//FOUO) Report No. DODIG-2015-048, "Joint Cyber Centers DoD OIG (b)(7)(E) Cyberspace Operations," December 8, 2014 (S//NF)

~~SECRET//NOFORN~~

(U) Management Comments

(U) Management Comments

(U) U.S. Cyber Command



~~SECRET//NOFORN~~
DEPARTMENT OF DEFENSE
UNITED STATES CYBER COMMAND
5600 SAVAGE ROAD, SUITE 6171
FORT GEORGE G. MEADE, MARYLAND 20755

OCT 14 2015

Reply to:
Commander

MEMORANDUM FOR THE INSPECTOR GENERAL, DEPARTMENT OF DEFENSE

Through: DIRECTOR OF THE JOINT STAFF

SUBJECT: (U//~~FOUO~~) Response to report: Combat Mission Teams and Cyber Protection
Teams Lacked Adequate Capabilities and Facilities to Perform Missions (Report
No. DODIG-2015-0059)

1. (U) United States Cyber Command (USCYBERCOM) appreciates the opportunity to respond to the subject DoDIG report and provides the following response to recommendations one, two, and three.

2. (U) Recommendation One. The DoDIG report recommends that Chiefs of Staff for the, U.S. Army and U.S. Air Force; Chief of Naval Operations; the Commandant of the Marine Corps; and the Commander, U.S. Cyber Command develop or update a doctrine, organization, training, materiel, leadership and education, personnel, facilities, and policy (DOTMLPF-P) framework to document capability requirements and associated capability gaps to build the current force, grow and mature the full Cyber Mission Force (CMF), and develop and sustain CMF capabilities.

~~(S//NF)~~ ARMY; USAF; USMC: (b)(1), Sec. 1.4(g)
ARMY; USAF; USMC: (b)(1), Sec. 1.4(g)

b. ~~(S//NF)~~ ARMY; USAF; USMC: (b)(1), Sec. 1.4(g)
ARMY; USAF; USMC: (b)(1), Sec. 1.4(g)

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

(U) U.S. Cyber Command (cont'd)

~~SECRET//NOFORN~~

3. (U//~~FOUO~~) Recommendation Two. The Commander, USCYBERCOM; Chiefs of Staff for the U.S. Army and U.S. Air Force; the Chief of Naval Operations; and the Commandant of the Marine Corps should formalize an agreement to focus capability development on functional and mission areas consistent with the results of the mission alignment board.

(U//~~FOUO~~) USCYBERCOM agrees with Recommendation Two. It is important for the cyber force to have an integrated approach for capability development; USCYBERCOM would need to engage with OSD and Service Chiefs to coordinate and begin developing formal agreements to focus capability development and facilitate integrated development approaches. Limited acquisition authority as described in the draft FY16 National Defense Authorization Act, if received, would also support increased coordination of capability development on functional and mission areas consistent with the results of the mission alignment board.

4. (U//~~FOUO~~) Recommendation Three. The Commander, USCYBERCOM, in coordination with the Service Components and DISA, should develop and specify a capability baseline and interoperability standards for Cyber Protection Teams (CPTs).

(S//~~FOUO~~) ~~ARMY; USAF; USMC; (b)(1), Sec. 1.4(g)~~
~~ARMY; USAF; USMC; (b)(1), Sec. 1.4(g)~~

5. (U//~~FOUO~~) The USCYBERCOM POC for this action is ~~DoD OIG: (b)(6)~~
~~DoD OIG: (b)(6)~~




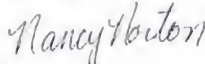
MICHAEL S. ROGERS
Admiral, U.S. Navy
Commander

Copy to:
Commander, USSTRATCOM

~~SECRET//NOFORN~~

(U) Management Comments

(U) Chief of Naval Operations

	SECRET
	UNCLASSIFIED UPON REMOVAL OF ENCLOSURE (1)
DEPARTMENT OF THE NAVY <small>OFFICE OF THE CHIEF OF NAVAL OPERATIONS 2000 Navy Pentagon Plaza Washington, DC 20380-5001</small>	
	1210 Ser N2N6F/S55119062 October 30, 2015
DoD OIG: (b)(6)	
Readiness and Cyber Operations 4800 Mark Center Drive Alexandria, VA 22350-1500	
Dear DoD OIG: (b)(6)	
(U) Enclosure (1) is the Navy response to the Department of Defense Inspector General draft audit report on the subject of "Combat Mission Teams and Cyber Protection Teams Lacked Adequate Capabilities and Facilities to Perform Missions" (Project No. D2015-D000RC-0059.000) dated 17 September 2015.	
(U) The Navy appreciates the opportunity to respond to the draft report. My point of contact is DoD OIG: (b)(6)	
Sincerely,  Nancy Norton Rear Admiral, U.S. Navy Director, Warfare Integration	
Enclosure 1 N2N6F Responses to DODIG Recommendations Project No. D2015-D000RC-0059.000) of 17 Sep 15	
Derived from: Multiple Sources Declassify on: SECRET	
SECRET UNCLASSIFIED UPON REMOVAL OF ENCLOSURE (1)	

~~SECRET//NOFORN~~

(U) Chief of Naval Operations (cont'd)



~~SECRET~~

DEPARTMENT OF THE NAVY
OFFICE OF THE CHIEF OF NAVAL OPERATIONS
2000 NAVY PENTAGON
WASHINGTON, DC 20350-2000

1210
Ser N2N6F3/S5S119062
October 30, 2015

From: Director, Warfare Integration (OPNAV N2/N6F)
To: Deputy Assistant Inspector General Readiness and Cyber Operations
Subj: (U//~~FOUO~~) NAVY RESPONSE TO DODIG RECOMMENDATIONS PROJECT NO.
D2015-D000RC-0059.000) DATED 17 SEPTEMBER 2015.

Reference: (a) ~~FOUO~~ DODIG Draft Audit Report of 17 Sep 15
(b) (U) Naval Inspector General Audit Liaison Manual § 0514
(c) (U) Department of Defense INSTRUCTION 7650.03

1. (U//~~FOUO~~) In response to reference (a) and in accordance with references (b) and (c), the following input is provided to subject report:

• (U) Recommendation 1

(U) We recommend the Chiefs of Staff for the U.S. Army and U.S. Air Force; the Chief of Naval Operations; the Commandant of the Marine Corps; and the Commander U.S. Cyber Command develop a Doctrine, Organization, Training, Material, Leadership and Education, Personnel, Facilities and Policy (DOTMLP-F) framework that addresses strategies to build grow and sustain the Cyber Mission Force.

(U//~~FOUO~~) Navy Position: NAVY: (b)(7)(E)

• (U) Recommendation 2

(U) We recommend the Commander, U.S. Cyber Command, and the Chiefs of Staff for the U.S. Army and U.S. Air Force, the Chief of Naval Operations and the Commandant of the Marine Corps formalize an agreement to focus capability development on functional and mission areas consistent with the results of mission alignment board.

Derived from: USCCI 5200-07
Declassify on: ~~SECRET~~

~~SECRET~~

(U) Chief of Naval Operations (cont'd)

~~SECRET~~

~~SECRET~~ ARMY; NAVY; USAF; USMC; (b)(1), Sec. 1.4(g)



- (U) Recommendation 3

(U) We recommend the Commander, U.S. Cyber Command, in coordination with the Service Components and the Defense Information Systems Agency, develop and specify a capability baseline and interoperability standards for all Cyber Protection Teams (CPT)

~~SECRET~~ ARMY; NAVY; USAF; USMC; (b)(1), Sec. 1.4(g)



N. A. Norton
N. A. NORTON
Rear Admiral, U.S. Navy

2
~~SECRET~~

(U) U.S. Army Chief of Staff



~~SECRET//NOFORN~~
DEPARTMENT OF THE ARMY
OFFICE OF THE DEPUTY CHIEF OF STAFF, G-3/5/7
3200 ARMY PENTAGON
WASHINGTON, DC 20310-3200

DAMO-ODCI

16 October 2015

MEMORANDUM FOR Department of Defense (DoD) Inspector General (IG), ATTN: ~~DoD OIG; (b)(6)~~
~~DoD OIG; (b)(6)~~ Readiness and Cyber Operations, 4800 Mark
Center Drive, Alexandria, Virginia 22350-1500

SUBJECT: (U//~~FOUO~~) Army Comments to DoDIG Draft Report: "(U//~~FOUO~~) Combat
Mission Teams and Cyber Protection Teams (CPTs) Lacked Adequate Capabilities and
Facilities to Perform Missions" (D2015-D000RC-0059.000) dated 17 September 2015
(S//NOFORN)

1. General Comments:

- a. ~~(S//REL TO USA, FVEY)~~ DoDIG comment: ARMY, USAF, USMC: (b)(1), Sec. 1.4(g)

[Redacted]

- b. ~~(S//REL TO USA, FVEY)~~ Army Response: ARMY, USAF, USMC: (b)(1), Sec. 1.4(g)

[Redacted]

¹ CJCS Memorandum, 5 December 2012, subject: 30 Nov JCS Tank on CYBERCOM Mission Manpower

~~SECRET//NOFORN~~

(U) U.S. Army Chief of Staff (cont'd)

~~SECRET//REL USA, FVEY~~

ARMY; USAF; USMC: (b)(1), Sec. 1.4(g)



2. DODIG Recommendations:

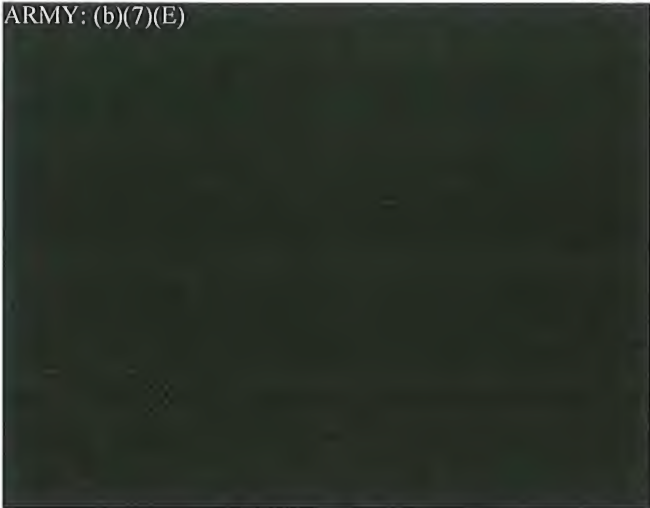
- a. **(U) Recommendation 1:** We recommend the Chiefs of Staff for the U.S. Army and U.S. Air Force; the Chief of Naval Operations; the Commandant of the Marine Corps; and the Commander, U.S. Cyber Command **develop a doctrine, organization, training, materiel, leadership and education, personnel, facilities, and policy (DOTMLPF-P) framework that address strategies to build, grow, and sustain the Cyber Mission Force.**
- b. **(U//~~FOUO~~) Army Response:** Concur. There is a need to conduct a collaborative Joint Services assessment across the entire DOTMLPF-P that focuses on integrating efforts and strategies to support building, growing, and sustaining the Cyber Mission Force (CMF). This approach would allow Services to share their independent assessments, help determine cross-cutting capabilities and foster innovative approaches. The Army is developing a comprehensive Cyberspace Strategy that presents the Army vision for cyberspace, end states, and major objectives to integrate all Army activities and operations in cyberspace and the information environment. This strategy

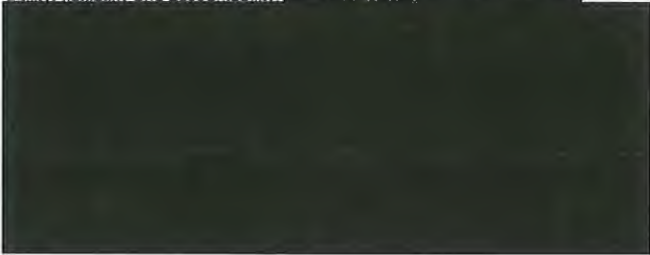
~~SECRET//REL USA, FVEY~~

(U) U.S. Army Chief of Staff (cont'd)

~~SECRET//REL USA, FVEY~~

ARMY: (b)(7)(E)



- c. (U) **Recommendation 2:** We recommend the Commander, U.S. Cyber Command, and the Chiefs of Staff for the U.S. Army and U.S. Air Force, the Chief of Naval Operations, and the Commandant of the Marine Corps **formalize an agreement to focus capability development on functional and mission areas consistent with results of the mission alignment board.**
- d. (U//~~FOUO~~) **Army Response:** Concur. The Army requires a proactive governance and management construct to rapidly deliver cyber capabilities with agility, flexibility and accountability. ARMY: (b)(7)(E)
- 

~~SECRET//REL USA, FVEY~~

(U) U.S. Army Chief of Staff (cont'd)

~~SECRET//NOFORN~~

ARMY: (b)(7)(E)

3. The Headquarters, Department of the Army, ODCI G-39, point of contact is DoD OIG: (b)(6)
DoD OIG: (b)(6)



CARMINE CICALESE
COL, GS
Chief, Cyberspace and Information Operations
Division

~~SECRET//NOFORN~~

(U) U.S. Army Cyber Command and Second Army



UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

DEPARTMENT OF THE ARMY
U.S. ARMY CYBER COMMAND AND SECOND ARMY
8825 BEULAH STREET
FORT BELVOIR, VIRGINIA 22060-5248

ARCC-IR

16 OCT 2015

MEMORANDUM FOR Department of Defense (DoD) Inspector General (IG), ATTN: ~~DoD OIG: (b)(6)~~
DoD OIG: (b)(6) Readiness and Cyber Operations, 4800 Mark
Center Drive, Alexandria, Virginia 22350-1500

SUBJECT: (U//~~FOUO~~) Command Comments to DoDIG Draft Report: "(U//~~FOUO~~) Combat
Mission Teams and Cyber Protection Teams Lacked Adequate Capabilities and Facilities to
Perform Missions" (D2015-D000RC-0059.000) dated 17 September 2015 (S//NOFORN)

1. (U) U.S. Army Cyber Command (ARCYBER) reviewed the subject draft report and your
recommendation: "(U) RECOMMENDATION 4: (U) We recommend the Commander,
Army Cyber Command and Second Army develop a time-sensitive plan of action and
milestones to provide all Army Cyber Protection Teams with adequate workspace and
ARMY: (b)(7)(E)

2. (U) We concur. The Network Enterprise Technology Command (NETCOM) staff are
currently working with the Cyber Protection Brigade (CPB) to assist in resourcing facilities
and network improvements. During the course of the audit, ARCYBER and NETCOM
completed the full facility and network analysis on capabilities needed for the CPB and
developed a plan of action and milestones to provide all Army Cyber Protection Teams
(CPTs) with adequate workspace ARMY: (b)(7)(E)

3. (U) If you have any questions, please contact DoD OIG: (b)(6)
DoD OIG: (b)(6)

EDWARD C. CARDON
Lieutenant General, USA
Commanding

CF:
HQDA (DAMO-ODCI)
HQDA (SAAG-ACFO)

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

~~SECRET//NOFORN~~

(U) Management Comments

(U) U.S. Marine Corps Forces Cyber Command



UNCLASSIFIED//FOR OFFICIAL USE ONLY

UNITED STATES MARINE CORPS
U. S. MARINE CORPS FORCES CYBERSPACE COMMAND
3800 SAVAGE ROAD SUITE 6850
FORT MEADE MARYLAND 20755

IN REPLY REFER TO:
1000
CDR
OCT 20 2015

From: Commander, U.S. Marine Corps Forces Cyberspace Command (MARFORCYBER)
To: Inspector General, U.S. Department of Defense
Via: Director, Marine Corps Staff

Subj: [U//~~FOUO~~] DRAFT DODIG REPORT D2015-0000RC-0059.000 "COMBAT MISSION
TEAMS AND CYBER PROTECTION TEAMS LACKED ADEQUATE CAPABILITIES AND
FACILITIES TO PERFORM MISSIONS," DATED SEPTEMBER 17, 2015
(SECRET//NOFORN)

Encl: (1) (U) MARFORCYBER RESPONSES TO RECOMMENDATIONS (S//REL)
(2) (U) MARFORCYBER SECURITY MARKING REVIEW (S//REL)

1. (U) PURPOSE. To transmit the approved MARFORCYBER comments pertaining to the Draft DoDIG report D2015-0000RC-0059.000 "Combat Mission Teams and Cyber Protection Teams Lacked Adequate Capabilities and Facilities to Perform Missions."

2. (U//~~FOUO~~) BACKGROUND. The Office of the Inspector General, Department of Defense, provided draft report D2015-0000RC-0059.000, "Combat Mission Teams and Cyber Protection Teams Lacked Adequate Capabilities and Facilities to Perform Missions" dated September 17, 2015 to MARFORCYBER for review and comment. Instructions are for MARFORCYBER to provide comments on whether leadership agrees (concur) or disagrees (non-concur) with the findings and recommendations in the report. MARFORCYBER was instructed to specifically answer recommendations one, two, and if desired three. Additionally, the command has been directed to review all classification markings of the report and our response.

3. (U) DISCUSSION

- a. (U) Recommendation 1. MARFORCYBER concurs; see enclosure (1).
- b. (U) Recommendation 2. MARFORCYBER non-concurs; see enclosure (1).
- c. (U) Recommendation 3. MARFORCYBER concurs; see enclosure (1).
- d. (U) Security Marking Review. Completed; see enclosure (2).

4. (U//~~FOUO~~) Point of contact for this matter is DoD OIG: (b)(6)
DoD OIG: (b)(6)

L. E. Reynolds
L. E. REYNOLDS

UNCLASSIFIED//FOR OFFICIAL USE ONLY

~~SECRET//NOFORN~~

(U) U.S. Marine Corps Forces Cyber Command (cont'd)

~~SECRET//NOFORN~~
DODIG DRAFT AUDIT REPORT DATED SEPTEMBER 17, 2015
PROJECT NO. D2015-D000RC-0059.000

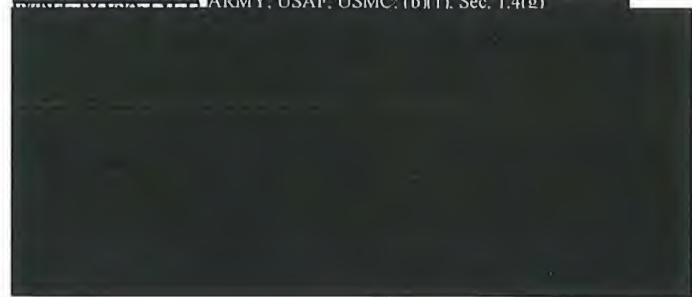
"COMBAT MISSION TEAMS AND CYBER PROTECTION TEAMS LACKED ADEQUATE CAPABILITIES AND FACILITIES TO PERFORM MISSIONS"

U.S. MARINE CORPS COMMENTS TO THE DODIG RECOMMENDATIONS

RECOMMENDATION 1: DODIG recommends that the Chiefs of Staff for the U.S. Army and U.S. Air Force; the Chief of Naval Operations; the Commandant of the Marine Corps; and the Commander, U.S. Cyber Command develop a doctrine, organization, training, materiel, leadership and education, personnel, facilities, and policy framework that address strategies to build, grow, and sustain the Cyber Mission Force.

COMMANDANT OF THE MARINE CORPS RESPONSE:

~~SECRET//NOFORN~~ ARMY: USAF: USMC: (b) (1), Sec. 1.4(g)



RECOMMENDATION 2: DODIG recommends that the Chiefs of Staff for the U.S. Army and U.S. Air Force; the Chief of Naval Operations; the Commandant of the Marine Corps; and the Commander, U.S. Cyber Command formalize an agreement to focus capability development on functional and mission areas consistent with results of the mission alignment board.

COMMANDANT OF THE MARINE CORPS RESPONSE:

(U//~~FOUO~~) Non-concur. The ability to focus capability development is a joint objective and should be led by the Combatant Commander, USSTRATCOM or a delegated representative (e.g., USCYBERCOM). No formalized agreement is required; the appropriate mechanism would be the issuance of an order (i.e., TASKORD, FRAGO, OPORD). The Mission Alignment Board (MAB) process is only relevant to Combat Mission Teams and National Mission Teams and does not provide appropriate criteria for capability development of the Cyber Protection Force (CPF).

Classified By ~~SECRET//NOFORN~~
Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20161011

ENCLOSURE (1)

(U) U.S. Marine Corps Forces Cyber Command (cont'd)

~~SECRET//NOFORN~~

RECOMMENDATION 3: DODIG recommends that Commander, U.S. Cyber Command, in coordination with the Service Components and the Defense Information Systems Agency, develop and specify a capability baseline and interoperability standards for all Cyber Protection Teams.

COMMANDANT OF THE MARINE CORPS RESPONSE:

(U//~~FOUO~~) Concur. MARFORCYBER agrees that there should be a capability baseline and interoperability standard for the CPF. The standard should consider today's operating environment and the future Joint Information Environment (JIE) and should be codified in the Cyber Force Concept of Employment (CFCOE) or other directive documents. The standard should be established using a functional and mission analysis of CPT operations. It should specify a minimum capability, but not limit CPTs from exceeding the standard when necessary and where possible. Given the evolutionary nature of the operating environment, the baseline standard must not restrict CPTs from adapting their tools and methodology to meet emerging threats. I recommend the baseline identify functions or capabilities rather than specific tools. Finally, the creation of an acceptable tools list with a universal authority to operate (ATO) on any DoDIN network, or portion thereof, would provide teams flexible options, enabling rapid implementation and increasing operational tempo for incident response forces.

~~SECRET//NOFORN~~

ENCLOSURE (1)

(U) U.S. Air Forces Cyber Command and 24th Air Force



~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~
DEPARTMENT OF THE AIR FORCE
HEADQUARTERS 24TH AIR FORCE (AIR FORCES CYBER) (AFSPC)
JOINT BASE SAN ANTONIO - LACKLAND TEXAS

19 October 2015

MEMORANDUM FOR Office of the Inspector General Department of Defense

FROM: 24AF/CC
3515 S. General McMullen Drive
Joint Base San Antonio - Lackland TX 78226-9853

SUBJECT: Draft Report for Project No. D2015-D000RC-0059.000

1. (U//~~FOUO~~) PURPOSE. Obtain 24 AF/CC coordination and approval of 24 AF comments pertaining to the Draft Report for Project No. D2015-D000RC-0059.000

2. (U//~~FOUO~~) BACKGROUND. The Office of the Inspector General Department of Defense, issued the draft report for Project No. D2015-D000RC-0059.000, "Combat Mission Teams and Cyber Protection Teams Lacked Adequate Capabilities and Facilities to Perform Missions" dated September 17, 2015 for 24 AF review and comment. Instructions are for 24 AF to provide comments on whether management agrees or disagrees with the finding and recommendations in the report. If in agreement 24 AF is instructed to describe what actions have been taken or planned to accomplish the recommendations including the completion dates. If in disagreement, 24 AF is instructed to give specific reasons for disagreement and propose alternative action if appropriate.

3. DISCUSSION. 24 AF concurs with comments.

a. (U) DoD IG Recommendation 1

(U) We recommend the Chiefs of Staff for the U.S. Army and U.S. Air Force; the Chief of Naval Operations; the Commandant of the Marine Corps; and the Commander, U.S. Cyber Command develop a doctrine, organization, training, materiel, leadership and education, personnel, facilities, and policy framework that address strategies to build, grow, and sustain the Cyber Mission Force.

(U) 24 AF/AFCYBER response:

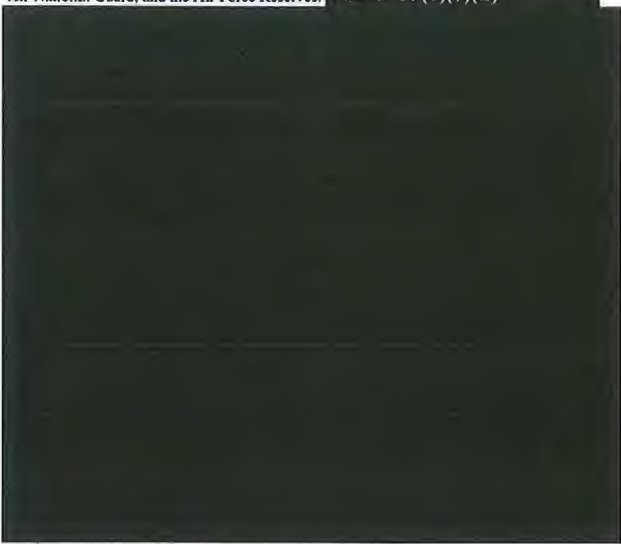
(U//~~FOUO~~) The 24 AF/AFCYBER will continue to work with HQ USAF, and USCYBERCOM to develop or update a DOTMLPF&P framework. The organizations will continue to document capability requirements and associated capability gaps to build the current force, grow and mature the full CMF, and develop and sustain CMF capabilities. The AFSPC Project Task Force (PROTAF) has already made progress towards institutionalizing the DOTMLPF framework and has produced strategic level doctrinal framework including:

- (U//~~FOUO~~) The CMF Program Action Directive (PAD), dated 15 Jan 2014, established DOTMLPF guidance for the AF CMF build. The PAD established planning actions across training, budget, facilities, equipment, personnel and total force (Air Force Reserves (AFR) and Air National Guard (ANG)) lines of effort. The execution arm of our DOTMLPF effort and PAD guidance is the Project Task Force (PROTAF) which consists of membership from AFCYBER, AFCYBER_FWD, Air Force Space Command, Headquarters Air Force (HAF),

(U) U.S. Air Forces Cyber Command and 24th Air Force (cont'd)

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

Air National Guard, and the Air Force Reserves. DoD OIG: (b)(7)(E)



Date of Completion: Multiple, ongoing actions until full FOC build.

b. (U) DoD IG Recommendation 2

(U) We recommend the Commander, U.S. Cyber Command, and the Chiefs of Staff for the U.S. Army and U.S. Air Force, the Chief of Naval Operations, and the Commandant of the Marine Corps formalize an agreement to focus capability development on functional and mission areas consistent with results of the mission alignment board.

(U) 24 AF/AFCYBER response:

(U//~~FOUO~~) The 24 AF/AFCYBER will continue to work with HQ USAF, USCYBERCOM and other CMF oversight bodies such as the CMF rDT Technical Oversight Council, in accordance with the Cyber Force Concept of Employment (CFCOE) directive, to formalize agreements that allow Combatant Commanders, guided by the Mission Alignment Board, to direct capability development that support the Combatant Commander's mission requirements and priorities.

(U) Date of Completion: On-going activity

4. (U) VIEWS OF OTHERS.

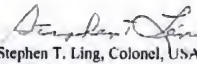
NA

(U) U.S. Air Forces Cyber Command and 24th Air Force (cont'd)

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

5. (U) RECOMMENDATION. AFCYBER concurs with comments to Draft Report for Project No. D2015-D000RC-0059.000 (Tab 1).

6. (U) My subject matter expert is DoD OIG: (b)(6)
DoD OIG: (b)(6)


Stephen T. Ling, Colonel, USAF
Chief of Staff *for CC*

1 Tabs

Tab 1 – DoDIG Draft Report for Project No. D2015-D000RC-0059.000

(U) Source of Classified Information

Source 1: (U) Deputy Secretary of Defense Memorandum, "Resource Management Decisions for FY 2014 Budget Request:" S//NF

Declassification Date: April 10, 2038

Generated Date: April 10, 2013

Source 2: (U) USCYBERCOM Cyber Force Concept of Operations and Employment, Version 4.1: S//REL TO USA, FVEY

Declassification Date: August 1, 2039

Generated Date: July 22, 2014

Source 3: (U//~~FOUO~~) USCYBERCOM Task Order 13-0244, "Establishment and Presentation of CMF Teams in FY 2013:" S//REL TO USA, FVEY

Declassification Date: March 6, 2038

Generated Date: March 6, 2013

Source 4: (~~S//REL TO USA, FVEY~~) ARMY; USAF; USMC: (b)(1), Sec. 1.4(g)

Declassification Date: October 11, 2038

Generated Date: October 11, 2013

Source 5: (~~S//REL TO USA, FVEY~~) ARMY; USAF; USMC: (b)(1), Sec. 1.4(g)

Declassification Date: May 13, 2038

Generated Date: May 13, 2013

Source 6: (~~S//REL TO USA, FVEY~~) ARMY; USAF; USMC: (b)(1), Sec. 1.4(g)

Declassification Date: April 5, 2037

Generated Date: April 5, 2012

Source 7: (~~S//NF~~) ARMY; USAF; USMC: (b)(1), Sec. 1.4(g)

Declassification Date: May 19, 2038

Generated Date: May 19, 2013

Source 8: (~~S//REL TO USA, FVEY~~) ARMY; USAF; USMC: (b)(1), Sec. 1.4(g)

Declassification Date: June 30, 2038

Generated Date: March 30, 2015

~~SECRET//NOFORN~~

(U) Source of Classified Information

Source 9: (~~S//REL TO USA, FVEY~~) ARMY; USAF; USMC: (b)(1), Sec. 1.4(g)

Declassification Date: August 1, 2039

Generated Date: August 14, 2014

Source 10: (~~S//NF~~) ARMY; USAF; USMC: (b)(1), Sec. 1.4(g)

Declassification Date: November 1, 2039

Generated Date: November 20, 2014

Source 11: (U) Deputy Secretary of Defense Memorandum, "Resource Management Decisions for FY 2016 Budget Request:" S//NF

Declassification Date: December 10, 2039

Generated Date: December 10, 2014

Source 12: (~~S//NF~~) ARMY; USAF; USMC: (b)(1), Sec. 1.4(g)

Declassification Date: June 25, 2040

Generated Date: June 25, 2015

Source 13: (~~S//REL TO USA, FVEY~~) ARMY; USAF; USMC: (b)(1), Sec. 1.4(g)

Declassification Date: July 19, 2038

Generated Date: May 1, 2014

Source 14: (~~S//NF~~) ARMY; USAF; USMC: (b)(1), Sec. 1.4(g)

Declassification Date: August 1, 2039

Generated Date: October 22, 2012 (updated November 20, 2012)

Source 15: (~~S//REL TO USA, FVEY~~) ARMY; USAF; USMC: (b)(1), Sec. 1.4(g)

Declassification Date: December 19, 2039

Generated Date: January 9, 2015

Source 16: (U) Request for Initial Operational Capability Designation - ~~DoD OIG: (b)(7)(E)~~
S//REL TO USA, FVEY

Declassification Date: September 13, 2038

Generated Date: September 13, 2013

Source 17: (U) 400 CMT Initial Operational Capability Designation:
S//REL TO USA, FVEY

Declassification Date: October 9, 2039

Generated Date: October 9, 2014

~~SECRET//NOFORN~~

Source 18: (U) 600 CMT Initial Operational Capability Declaration:

S//REL TO USA, FVEY

Declassification Date: April 18, 2039

Generated Date: April 18, 2014

Source 19: (U) 102 CMT Initial Operational Capability Declaration:

S//REL TO USA, FVEY

Declassification Date: July 1, 2039

Generated Date: April 1, 2014

Source 20: (U) OSD Cost Assessment and Program Evaluation, "Cyber Issue Team

Deputy's Management Advisory Group Comeback:" S//NF

Declassification Date: August 31, 2033

Generated Date: December 11, 2012

Source 21: (U) USCYBERCOM Presentation on CMF Concept of Operations:

S//REL TO USA, FVEY

Declassification Date: December 11, 2037

Generated Date: January 16, 2014

Source 22: (~~S//REL TO USA, FVEY~~) ARMY; USAF; USMC: (b)(1), Sec. 1.4(g)

Declassification Date: January 12, 2040

Generated Date: January 12, 2015

Source 23: (~~S//REL TO USA, FVEY~~) ARMY; USAF; USMC: (b)(1), Sec. 1.4(g)

Declassification Date: February 1, 2039

Generated Date: January 8, 2007

Source 24: (U//~~FOUO~~) USCYBERCOM Presentation on CMF Funding: S//NF

Declassification Date: April 1, 2037

Generated Date: November 20, 2014

Source 25: (U) Memorandum of Agreement Between U.S. Army Intelligence and Security Command and 24th Air Force for Totem Stone Infrastructure and Advanced Cyberspace Operations Concepts, Tools, Techniques, and Technologies: S//NF

Declassification Date: November 21, 2038

Generated Date: December 9, 2013

Source 26: (U) Deputy Secretary of Defense Memorandum, "Follow-on Guidance from the April 18, 2015, Cyber Deep Dive:" S//REL TO USA, FVEY

Declassification Date: June 3, 2040

Generated Date: June 3, 2015

(U) Acronyms and Abbreviations

AFCYBER	Air Forces Cyber Command
ARCYBER	Army Cyber Command
CCR	Cyber Capabilities Registry
CMF	Cyber Mission Force
CMT	Combat Mission Team
CPT	Cyber Protection Team
CST	Combat Support Team
DISA	Defense Information Systems Agency
DoDIN	DoD Information Network
DOTMLPF-P	Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel, Facilities, and Policy
FLTCYBER	Fleet Cyber Command
GAO	Government Accountability Office
JFHQ	Joint Force Headquarters
JWICS	Joint Worldwide Intelligence Communications System
MARFORCYBER	Marine Corps Forces Cyber Command
NMT	National Mission Team
NST	National Support Team
NIPRNet	Non-Secure Internet Protocol Router Network
SCIF	Sensitive Compartmented Information Facility
SIPRNet	Secret Internet Protocol Router Network
SMO	Support to Military Operations
USCYBERCOM	U.S. Cyber Command

~~SECRET//NOFORN~~

Whistleblower Protection

U.S. DEPARTMENT OF DEFENSE

The Whistleblower Protection Enhancement Act of 2012 requires the Inspector General to designate a Whistleblower Protection Ombudsman to educate agency employees about prohibitions on retaliation, and rights and remedies against retaliation for protected disclosures. The designated ombudsman is the DoD Hotline Director. For more information on your rights and remedies against retaliation, visit www.dodig.mil/programs/whistleblower.

For more information about DoD IG reports or activities, please contact us:

Congressional Liaison

congressional@dodig.mil; 703.604.8324

Media Contact

public.affairs@dodig.mil; 703.604.8324

Monthly Update

dodigconnect-request@listserve.com

Reports Mailing List

dodig_report@listserve.com

Twitter

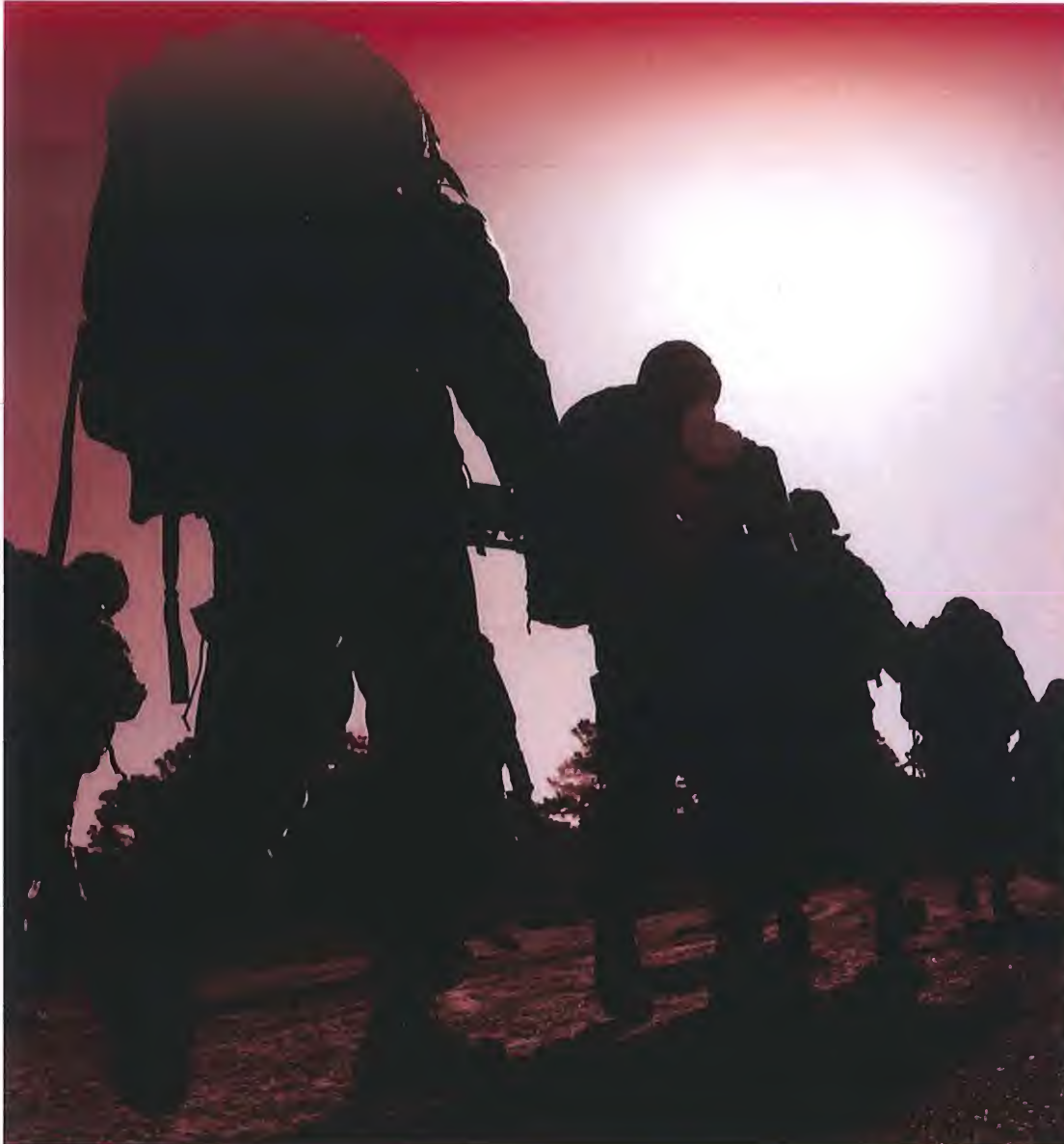
twitter.com/DoD_IG

DoD Hotline

dodig.mil/hotline

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~



DEPARTMENT OF DEFENSE | INSPECTOR GENERAL

4800 Mark Center Drive
Alexandria, VA 22350-1500
www.dodig.mil
Defense Hotline 1.800.424.9098

~~SECRET//NOFORN~~